INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2012/2013

TII

NOVAS FRONTEIRAS CRIADAS PELOS CIBERATAQUES. UM NOVO DESAFIO PARA A COOPERAÇÃO INTERNACIONAL

DOCUMENTO DE TRABALHO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS E DA GUARDA NACIONAL REPUBLICANA.

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

NOVAS FRONTEIRAS CRIADAS PELOS CIBERATAQUES. UM NOVO DESAFIO PARA A COOPERAÇÃO INTERNACIONAL

COR TM RUI MANUEL NUNES PINTO

Trabalho de Investigação Individual/CPOG 2012-13

Pedrouços 2013

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

NOVAS FRONTEIRAS CRIADAS PELOS CIBERATAQUES. UM NOVO DESAFIO PARA A COOPERAÇÃO INTERNACIONAL

Cor Tm Rui Manuel Nunes Pinto

Trabalho de Investigação Individual do CPOG 2012/13

Orientador:

Cor AdmAer João Carlos Bonifácio da Silva Matos

Coronel AdmAer

Pedrouços 2013

Agradecimentos

Ao meu orientador, o Coronel Cor AdmAer João Carlos Bonifácio da Silva Matos, pela disponibilidade e aconselhamento, que muito contribuíram para melhorar a clareza e a profundidade da investigação.

Às entidades entrevistadas, pela disponibilidade e pelos excelentes contributos para o esclarecimento e clarificação da problemática deste estudo.

Um agradecimento especial ao TCor Tm(Eng) Viegas Nunes pelos valiosos conhecimentos e sugestões que me transmitiu, fundamentais para a estruturação e enquadramento deste trabalho.

A todos os camaradas de curso que de alguma forma me deram os seus contributos, amizade e apoio neste desafio.

À minha família, Céu, Pedro e Sofia, ânimo da minha vida.

Índice

Índice de Anexos:

Indice de Apêndices

Índice de Tabelas

Índice de Figuras

Resumo

As sociedades modernas são caracterizadas por uma adesão intensiva às tecnologias de informação, que conjugadas com a utilização cada vez mais alargada da internet, têm gerado elevados índices de crescimento e qualidade de vida às populações.

A internet tem permitido a estruturação das sociedades em rede, e o estabelecimento de novas relações entre as pessoas, as organizações e os estados, contribuindo de forma inequívoca para a globalização e o mundo do conhecimento.

Concorrentemente, verifica-se o aparecimento, diariamente, de notícias nos media sobre a utilização ilícita da internet com fins criminosos, ou mesmo o aparecimento de novas tensões entre estados, resultantes de ciberameaças.

As Forças Armadas (FFAA) não só acompanharam a evolução tecnológica e inseriram nos seus sistemas a dimensão digital, como também desenvolveram capacidades para desempenhar um papel fundamental na proteção e defesa das sociedades digitais em rede, face às novas ciberameaças a que estão sujeitas.

Percebeu-se, no entanto, desde muito cedo, que as ameaças ao ciberespaço não têm fronteiras, evoluem muito rapidamente, são cada vez mais sofisticadas, causam danos de dimensão cada vez maior e exigem tempos de resposta cada vez mais curtas. Existe a consciência a nível mundial, de que se está perante um desafio em que só de forma partilhada e cooperativa, as organizações e os estados conseguirão atingir algum êxito na sua eliminação.

Este trabalho, num âmbito limitado às FFAA, pretende evidenciar alguns dos vetores de cooperação nas áreas da cibersegurança e na da ciberdefesa, que poderão ser aplicados e desenvolvidos. É realçado o facto de as FFAA terem que desenvolver essas linhas de cooperação, entre Ramos e destes com as organizações preocupadas com a ciberdefesa, como a Organização do Tratado do Atlântico Norte (NATO) e a União Europeia (UE), mas também com as demais estruturas nacionais e internacionais ligadas à cibersegurança.

Por último, são demonstradas algumas da áreas em que as FFAA têm que se desenvolver, para que de forma mais eficaz possam aumentar a cooperação no âmbito da ciberdefesa.

Abstract

Modern societies are characterized by an intensive adherence to information technology, which combined with the increasingly extensive use of the internet have generated high growth ratings and quality of life for the people.

The internet has allowed the structuring of corporate network, and establishing new relationships among people, organizations and states, unequivocally contributing to globalization and the world of knowledge.

Concurrently, there is the appearance of daily news in the media about the misuse of the internet for criminal purposes, or even the emergence of new tensions between states, resulting from cyber threats.

The Armed Forces not only kept pace with technological evolution and inserted into their systems the digital dimension, but also developed capabilities to play a key role in the protection and defense of companies in digital network, in face of new cyber threats they are subjected.

However, It was felt very early, that threats to cyberspace have no boundaries, evolve very rapidly, are increasingly sophisticated, their damage size keep increasing and require increasingly shorter response times. There is a global awareness that one is faced with a challenge, that organizations and States will manage to succeed in their elimination through sharing and cooperation.

This work, in a limited scope to Armed Forces, aims to highlight some of the vectors of cooperation in the areas of cyber security and cyber defense which may be developed and applied. It is stressed the fact that the Armed Forces have to develop the lines of cooperation between these branches not only with organizations concerned with cyber defense, as the North Atlantic Treaty Organization (NATO) and European Union (EU), but also with other national and international structures related to cyber security.

Finally, some of the areas where the Armed Forces have to develop so that they can more effectively enhance cooperation on cyber defense will be shown.

Palavras-Chave

Ciberataque, Ciberdefesa, Ciberespaço, Estratégia Nacional de Segurança da Informação, Infraestrutura Critica Nacional, Tecnologias da Informação e Comunicação.

Key-Words

Cyber attack, Cyber defense, Cyberspace, National Strategy for Information Security, National Critical Infrastructure, Information Technology and Communication.

Lista de abreviaturas, siglas e acrónimos

ACT	*Allied Command Transformation*
ALSIC	Administrador Local dos Sistemas de Informação e Comunicações
AM	Academia Militar
CCD COE	*Cooperative Cyber Defence Centre of Excellence*
CDMA	*Cyber-Defence Management Authority*
CEME	Chefe do Estado Maior do Exército
CERT	*Computer Emergency Response Team*
CIRC	*Computer Incident Response Capability*
CIRT	*Computer Incident Response Team*
CNA	*Computer Network Attack*
CNC	Centro Nacional de Cibersegurança
CND	*Computer Network Defense*
CNE	*Computer Network Exploitation*
CNO	*Computer Network Operations*
CPOG	Curso de Promoção a Oficial General
CRISI	Capacidade de Resposta a Incidentes de Segurança Informáticos
CRP	Constituição da Republica Portuguesa
CSI	Comunicações e Sistemas de Informação
CSIRT	*Computer Security Incident Response Team*
CYBERCOM	*Cyber Command*
CWID	Coalition Warrior Interoperability Demonstration
DCSI	Direção de Comunicações e Sistemas de Informação
DICSI	Divisão de Comunicações e Sistemas de Informação
DIH	Direito Internacional Humanitário
EISAS	*European Information Sharing and Alert System*
EMGFA	Estado-Maior-General das Forças Armadas
ENC	Estrutura Nacional de Cibersegurança
ENISA	European Network and Information Security Agency
EPT	Escola Prática de Transmissões
EUA	Estados Unidos da América
FCCN	Fundação para a Computação Cientifica Nacional
FFAA	Forças Armadas

FFCI	*Framework for Collaborative Interaction*
GE	*Guerra Eletrónica*
GNS	Gabinete Nacional de Segurança
HIP	Hipótese
IDS	*Intrusion Detetion System*
I&D	Investigação e Desenvolvimento
IEC	*International Electrotechnical Commission*
IO	*Information Operations*
IP	*Internet Protocol*
IRT	*Incident Response Team*
ISO	*International Organization for Standardization*
ISP	*Internet Service Providers*
ITU	*International Telecommunication Union*
IWS	*Internet World Stats*
JFCC	*Joint Functional Component Command*
JP	*Joint Publication*
LAN	*Local Area Network*
LCA	*Lei dos Conflitos Armados*
LDN	Lei da Defesa Nacional
LOBOFA	Lei Orgânica de Bases da Organização das Forças Armadas
MMHS	*Military Mensage Handling System*
NAC	*Network Access Control*
NATO	*North Atlantic Treaty Organisation*
NCIRC	*NATO Computer Incident Response Capability*
ONU	Organização das Nações Unidas
OSSIC	Oficial de Segurança dos Sistemas de Informação e Comunicações
PE	Porto Editora
QC	Questão Central
QD	Questão Derivada
RCM	Rede de Comunicações da Marinha
RCTS	Rede Ciência, Tecnologia e Sociedade
RDE	Rede de Dados do Exército
RFCM	Rede Fixa de Comunicações Militares
RTm	Regimento de Transmissões

SCADA	*Supervisory Control and Data Acquisition Systems*
SERT	*Security Response Team*
SI	Sistemas de Informação
SIC	Sistemas de Informação e Comunicações
SICA	Sistemas de Informação e Comunicações Automatizado
SIC-T	Sistemas de Informação e Comunicações Táticos
SIC-O	Sistemas de Informação e Comunicações Operacionais
SICOM	Sistema Integrado de Comunicações Militares
SoS	S*ystems of Systems*
STRATCOM	*US Strategic Command*
TII	Trabalho de Investigação Individual
TIC	Tecnologias de Informação e Comunicações
UE	União Europeia
USB	*Universal Serial Bus*
WAN	*Wide Area Network*
WEF	*World Economic Forum*

Introdução

A utilização intensiva da internet associada à rápida evolução tecnológica, levou ao aparecimento de novas formas de relacionamento entre as populações e as organizações, de forma transnacional, com possibilidades quase ilimitadas. Além da troca de informação, utilizando a infraestrutura de comunicações e os sistemas de informação, estes permitiram efetuar o comando, controlo e monitorização de sistemas críticos para as sociedades, como as redes de água, telecomunicações, transporte, sistemas financeiros, serviços de emergência e com grande destaque pela importância que têm, das redes de energia elétrica.

Paralelamente, utilizando os mesmos recursos tecnológicos ao dispor de todos, desenvolveram-se formas ilícitas de emprego do ciberespaço, tais como os ciberataques ou a recolha indevida de dados pessoais e das organizações, que se tornaram fonte de preocupações para as sociedades e um desafio para os estados modernos.

As FFAA são proprietárias de sistemas de informação e comunicações de segurança elevada, que são isolados das infraestruturas civis e dos correspondentes acessos à internet. Não se julgue, no entanto, que passam incólumes a esta realidade, pelo simples facto de partilharem apenas algumas das suas infraestruturas de comunicações menos criticas, com o mundo civil. As próprias FFAA poderão ser um alvo remunerador, pois debilita um dos seus organismos de defesa da soberania do país.

É neste contexto que assistimos ao aparecimento de organismos e de subdomínios infraestruturais nas FFAA nacionais e estrangeiras, assim como em entidades civis, com a preocupação de se protegerem e defenderem contra todos aqueles que à margem da lei, procuram obter dividendos financeiros ou competitivos, ou mesmo contra aqueles que ao tentarem desenvolver atividades disruptivas em infraestruturas críticas do País, colocam em causa a sua soberania.

Um aspeto a tomar-se em consideração nos ciberataques é que estes não têm fronteiras. As suas origens são quase sempre difíceis de identificar, sendo assim de vital interesse, que na luta contra as ciberameaças, mais do que nunca, os países e as suas organizações, trabalhem em cooperação. É para este objetivo que o presente trabalho de investigação pretende contribuir, tentando definir por um lado, os aspetos em que a cooperação poderá ser desenvolvida e, por outro, de que forma poderão ser desenvolvidas as competências no domínio da ciberdefesa, que atualmente já se encontram em fase de construção ou mesmo operacionais, no sentido de as tornar mais cooperativas.

Enunciado, Contexto e Base Conceptual.

O tema para o Trabalho de Investigação Individual (TII) tem o seguinte enunciado:

"Novas fronteiras criadas pelos ciberataques. Um novo desafio para a cooperação internacional".

Na era da informação e do conhecimento, a estruturação das sociedades em rede é uma das características que mais evidencia o grau de evolução do século XXI. Estar em rede e em particular através da internet, é para os indivíduos, organizações e estados, uma condição e uma necessidade não só para evoluírem, mas também para a própria sobrevivência no mundo atual.

A utilização maciça da internet por parte das populações facilitou ainda o acesso a bibliotecas e serviços, que de forma exponencial permitiram a partilha e o aumento do conhecimento.

A evolução tecnológica dos terminais, cada vez mais miniaturizados e evoluídos, conjugados com uma infraestrutura de comunicações mais rápida, levaram na última década ao aparecimento de serviços, que já se vislumbravam, mas que só agora se concretizam, disponíveis a qualquer cidadão ou organização, em qualquer parte do mundo.

Concorrentemente, no mesmo ambiente de grande evolução tecnológica e de fácil acesso, surgem atores que desenvolvem atividades de cariz ilegal ou criminoso, como a utilização de contas bancárias, sem autorização, o acesso a dados pessoais e de empresas de forma indiscriminada, o roubo de identidades, os ataques de negação de serviço a empresas e organismos e o ciberterrorismo, entre outros.

Os estados que já perceberam o impacto e a importância dos conflitos cibernéticos na sua defesa, desenvolveram e organizaram unidades militares de ciberguerra, com capacidades de monitorização, defesa e ataque, contando-se já nesta data mais de três dezenas de países com esta capacidade já publicitada. Perceciona-se que um novo espaço de conflito, com um potencial enorme, encontra-se em crescimento, urgindo que se desenvolvam por parte da sociedade, mecanismos que o permitam enfrentar.

Existem estudos, documentos e trabalhos de investigação que de alguma forma tentam delimitar os diversos aspetos de utilização do ciberespaço. Nesta vertente, os ciberataques são uma forma genérica para designar todos os tipos de ações intrusivas suportados no ciberespaço, com origem em indivíduos, organizações criminosas ou mesmo estados.

Interessa-nos neste trabalho de investigação, dar atenção aos ciberataques direcionados para as infraestruturas críticas e de defesa do País, no qual se inserem também as FFAA e neste contexto, fazer ressaltar os aspetos de cooperação internacional, que poderão exponenciar a ciberdefesa, entendendo-se esta como a luta contra os ciberataques.

Objeto de Estudo e sua delimitação.

No âmbito do presente estudo de investigação, houve que delimitar o seu campo de ação e alcance face ao espetro bastante largo de abrangência.

Pretende-se, essencialmente, determinar em que áreas e de que forma é possível realizar a cooperação na ciberdefesa, entre as FFAA e entidades exteriores a estas.

Embora já existam algumas formas de cooperação na cibersegurança e na ciberdefesa, entre organismos civis, nacionais e internacionais, delimitamos o nosso estudo àqueles que dizem respeito diretamente às FFAA e à análise da cooperação internacional desejável e possível com entidades como a NATO e a UE. Não deixamos de tentar perceber até aonde deverá ir esta cooperação, na medida em que a soberania nacional poderá, em determinadas condições de partilha, ser colocada em causa.

Desenvolvemos a investigação por duas vias: análise e avaliação da cooperação, que atualmente se realiza na ciberdefesa e, numa perspetiva de desenvolvimento, determinamos linhas de ação futuras, para uma cooperação mais efetiva entre as FFAA e os organismos internacionais.

Objetivos da investigação.

O objetivo desta investigação é determinar em que medida é possível desenvolver e eventualmente aumentar, a cooperação entre as FFAA e as organizações internacionais, na luta contra os ciberataques.

Esta meta tem implícito, um conjunto de objetivos específicos, de que se destacam os seguintes:

- Identificar claramente qual a capacidade atual de ciberdefesa das FFAA e em que medida permite a cooperação internacional.
- Clarificar quais as áreas de cooperação internacional de ciberdefesa pretendida pelas FFAA e quais as componentes a desenvolver, para que seja atingido este fim.

Pergunta de partida e questões derivadas.

Após várias consultas bibliográficas e contatos exploratórios sobre a temática desta investigação e em consonância com o método hipotético-dedutivo adotado pelo IESM deduziu-se a seguinte questão central: **"De que forma as FFAA poderão desenvolver e aumentar a cooperação internacional na ciberdefesa?"**

A resposta a esta questão levantou as seguintes questões derivadas:

QD1 – Qual é a capacidade de ciberdefesa já desenvolvida pelas FFAA?

QD2 – Como é que a capacidade de ciberdefesa já desenvolvida pelas FFAA, contribui para a cooperação internacional?

QD3 – Quais as áreas de cooperação internacional de ciberdefesa que são desejáveis pelas FFAA?

QD4 – Quais as componentes a desenvolver pelas FFAA que são necessárias para que se atinja a ciberdefesa cooperativa de forma desejável?

Para responder a estas questões derivadas, foram equacionadas as seguintes hipóteses, avaliadas no decorrer da investigação:

H1 – As FFAA dispõem de uma capacidade limitada na luta contra os ciberataques.

H2 – A cooperação entre as FFAA e outras organizações são reduzidas.

H3 – Os ciberataques, não tendo fronteiras, exigem a definição de áreas comuns de cooperação internacional.

H4 – As componentes a desenvolver no estabelecimento de uma ciberdefesa cooperativa internacional deverão permitir a partilha de informações técnicas, a normalização de procedimentos e a formação e treino.

Metodologia, percurso e instrumentos.

O percurso metodológico seguirá as sete etapas do método científico descrito por Quivy e Campenhoudt (Quivy e Camp, 1998).

Numa primeira etapa, após a leitura de um conjunto de documentos e consultas na internet e em bibliografia dedicada a esta temática, fixou-se a questão central, seguindo o método hipotético-dedutivo.

Seguiram-se duas etapas, a da exploração e o da fixação da problemática, com a finalidade de delimitar o âmbito do objeto da investigação de forma a torná-lo mais claro e evidente. Foram ainda realizadas ações exploratórias através de entrevistas a algumas personalidades com reconhecida competência ou responsabilidade na área de investigação.

Na quarta etapa, correspondente à construção do modelo de análise, articulamos os conceitos desenvolvidos, dados recolhidos, componentes e indicadores deduzidos, formulando as hipóteses.

A quinta etapa, a observação, com base nos indicadores subjacentes às dimensões dos conceitos de cada hipótese, foi consolidada, recorrendo quer à bibliografia específica, quer a consulta e entrevistas a militares experientes nesta temática e à recolha de novos dados.

Finalmente, seguiu-se a sexta etapa, análise das informações recolhidas e a validação ou refutação das hipóteses.

A investigação terminou com a redação das conclusões e das sugestões que permitirão propor linhas de ação, para novos desenvolvimentos futuros do tema investigado.

1. As capacidades de ciberdefesa das FFAA.

a. Caraterização das ameaças.

O ciberespaço está presente em todos os aspetos da vida quotidiana dos cidadãos, das organizações, dos estados, em todo o planeta de uma forma global. No acesso à internet através de um terminal de computador, numa chamada telefónica através de um telemóvel, na visualização de um programa de televisão digital, existem diversas maneiras de acedermos ao ciberespaço, de forma amigável, rotineira, com facilidade e naturalmente.

Os serviços disponibilizados são inúmeros e aumentam permanentemente. As vantagens em usufruir destas facilidades parecem evidentes e essenciais para a sobrevivência diária. A terminologia associada ao ambiente Web[1] é infindável; os *chats*[2], os *mails*, os *blogs*[3], o *Facebook*, o *e-learning*[4], o HI8, o *Goggle*, o *Twitter*, o *Flickr*, entre outros. Ouvimos notícias, lemos "*mails*", jogamos em rede, efetuamos compras, guardamos documentos, consultamos bibliotecas, comunicamos ideias, partilhamos fotografias e experiências diárias, construímos e participamos em espaços virtuais à escala planetária, sem quaisquer limites.

E é aqui, nesta utilização intensiva e sem preocupação, que existe um desfasamento entre o mundo do ciberespaço, eminentemente virtual, e o mundo real com os seus riscos e perigos. O cidadão comum quer acesso à Web de forma rápida, fiável, com grande capacidade de alojamento e transmissão de informação, relegando aspetos de segurança para um segundo plano. Acredita, na maioria dos casos, que uma simples *password* é suficiente para impedir a violação dos seus dados. Existe uma perceção, ainda que falsa, de que os operadores que lhe facilitam a utilização da Web, estarão preocupados com a proteção desses mesmos dados.

Assiste-se, no entanto, ao aparecimento de entidades que paralelamente utilizam e tiram partido desses mesmos dados, quase sempre sem o conhecimento dos cidadãos. "*Todos os que fizerem login na Web, colocam-se em um domínio que pode ser utilizada não só para fins produtivos, mas simultaneamente é uma área potencial, para fins criminais ou hostis*" (Alexander, 2010). Verifica-se que de forma organizada, diversos atores acedem aos dados pessoais e das empresas, obtendo informações confidenciais e sem autorização, dando-lhes vantagens financeiras e competitivas ilegais. Mais grave

[1] De *World Wide Web* também conhecido como *Web*.
[2] Aplicações de conversação em tempo real.
[3] *Sites* cuja estrutura permite a atualização rápida a partir de acréscimos, ou *posts*.
[4] Modelo de ensino à distância, em que os conteúdos são disponibilizados através da internet.

ainda, surgem grupos de ideologias politicas e convicções opostas à dos governos institucionais, que através da utilização do ciberespaço, acedem indevidamente a dados governamentais ou impedem mesmo o funcionamento desses mesmos organismos, através de ações de *activism*[5], *hacking*[6] ou mesmo ciberterrorismo, colocando em causa a segurança e a soberania de um país.

Estamos perante uma nova realidade, visível na figura nº1, que exponencia o risco social. Qualquer notícia pode passar de um lado ao outro do planeta de forma "viral" através da Internet, desequilibrando o bem-estar social de um país. Ou por outro lado, o impacto de uma ameaça cibernética pode ser tal, que altere o funcionamento das redes das infraestruturas criticas colocando em causa a segurança nacional.

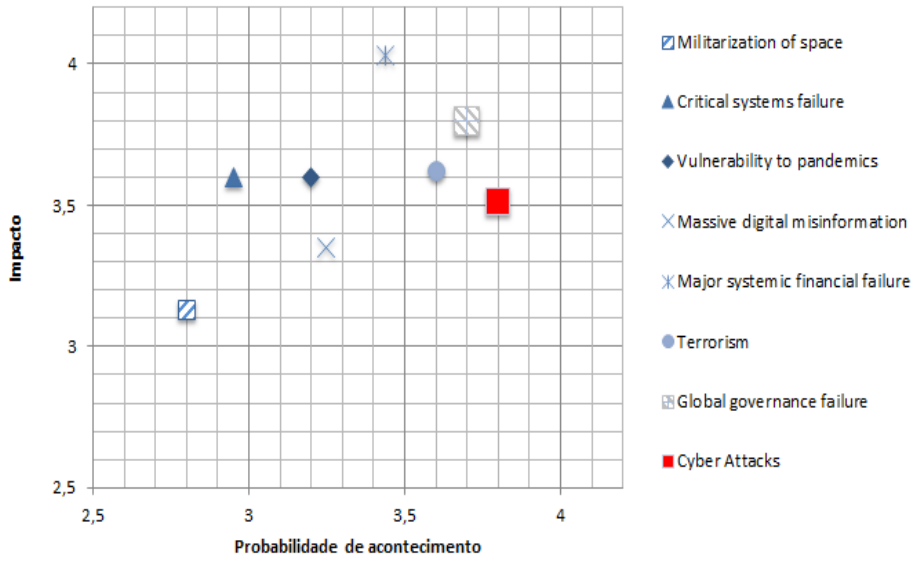


Figura nº1: Riscos globais próximos 10 anos

Fonte: (WEF, 2013) adaptado pelo autor

(1) Tipologia das ameaças.

Atualmente existe uma vasta panóplia de ciberataques, que não param de crescer pela quantidade e diversidade e dos quais temos conhecimento diariamente através dos *média* e da literatura especializada. "*Roubo de informação, interceção ou adulteração de*

[5] Atividades desenvolvidas por grupos ou comunidades que pretendem influenciar a política externa de determinado país ou países, através da *internet.*

[6] Atividades com o objetivo de modificar ou alterar programas ou sistemas de informação, de forma não autorizada. Mais recentemente, os indivíduos que se dedicam a esta atividade, os hackers, têm sido também contratados pelas empresas, para que de forma legal, desenvolvam e melhorem a segurança de novos programas.

comunicações (telefones, mail) e possibilidade de comprometer sistemas (ganhar controlo sobre eles), são os grandes grupos de vulnerabilidades encontrados pelo Vigilis[7]*, que podem ser detalhadas em 19 tipos diferentes*" (Expresso,2011). A lista de ameaças é interminável; *spam*[8], ataque DOS[9], ações de *phishing*[10], *spoofings*[11], *floodings*[12], entre outros, que podem ser organizados em ataques de validação, de negação de serviços, de modificação ou até de "simples" monitorização. Por detrás destas ações, milhares de grupos e de comunidades, com mais ou menos conhecimento das TIC, motivados pelas mais diferentes razões, de forma ilícita tentam tirar vantagens do ciberespaço. Aqui encontramos os *hackers*[13], os *insiders*[14] e todos aqueles os que desenvolvem o *activism*, o *hacktivism*[15], a ciberespionagem e até o ciberterrorismo.

Na tabela 1 mostram-se algumas das ameaças ao ciberespaço mais recorrentes e os seus agentes típicos. Repare-se como a obtenção de informação confidencial e o seu uso é uma ameaça desenvolvida por todos os agentes.

Tabela 1:Tipificação das ameaças cibernéticas em 2012

Fonte: (ENISA, 2012b) adaptado pelo autor

	Agentes de Ameaça					
Ciberataques	**Empresas**	**Ciber-criminosos**	**Empregados**	**Hactivistas**	**Estados**	**Terroristas**
Drive-By Exploits		•				•
Worms/trojans		•			•	•
Code Injection		•		•		•
Exploit Kits		•				
Botnets	•	•		•		•
Denial Of Service		•		•	•	•
Pishing Attacks		•				
Compromising Confidential Information	•	•	•	•	•	•
Rogueware/Scareware		•			•	
Spam	•	•				
Targeted Attacks	•	•			•	•
Physical Theft / Loss / Damage	•	•	•		•	•
Identity Theft	•	•	•		•	
Abuse of Information Leakage	•	•	•	•	•	•
Search Engine Poisoning	•	•				
Rogue Certificates		•			•	

[7] O Vigilis é um sistema de vigia das redes de informática da Universidade de Coimbra.
[8] Mensagem eletrónica não solicitada e enviada em massa, geralmente com fins publicitários.
[9] *Denial of Service* (DOS) ataque de negação de serviço.
[10] Fraude eletrónica para obter: senha, dados financeiros e outros dados pessoais.
[11] Ataque usando identidade de um utilizador, para obter dados e informações de uma rede.
[12] Ataque que consiste numa inundação de pedidos, saturando a máquina vitima.
[13] Individuo que se dedica explorar e alterar programas, dispositivos e redes de PCs ligados à internet.
[14] Individuo que realiza atividades ilícitas no seu local de trabalho, com o uso dos seus conhecimentos informáticos.
[15] Atividade resultante do *activism* com o *hacking*.

A figura 2 mostra quais as motivações que estão por detrás dos ciberataques.

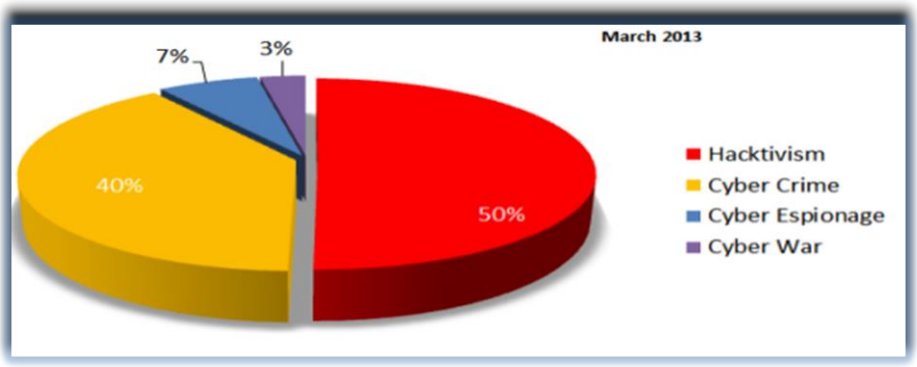


Figura nº 2: Motivações dos ciberataques

Fonte:(Hackmageddon, 2013)

Uma das pragas mais disseminadas que estão a exigir mais recursos para debelar a nível internacional atualmente, são os "*botnets*". Este termo pode ser utilizado para designar um grupo de "*bots*"[16], mas geralmente é usado para designar um conjunto de computadores comprometidos onde o software malicioso permanece em execução. Remotamente o cibercriminoso controla as máquinas contaminadas, que podem atingir rapidamente os milhares, permitindo o envio de *spam* ou desenvolver uma ciberameaça em larga escala, a troco de dinheiro ou outro proveito ilícito. Neste grupo situam-se também ações de ciberespionagem e a possibilidade muito real de se desenvolverem ações de ciberterrorismo em larga escala.

No grupo dos que dão maiores preocupações à comunidade internacional estão também o zero days vírus[17]. A "*Kaspersky Lab publicou uma pesquisa revelando que poucos internautas acompanham as novas descobertas sobre ameaças online. Apenas 11% sabe o que é ataque Day Zero e quase metade dos entrevistados já haviam sido afetados diretamente por esse tipo de golpe*" (Canaltech, 2013).Esta praga só se torna evidente à segurança das redes de informática depois de se manifestar, ultrapassando as barreiras de proteção e causando sempre danos avultados às empresas e às organizações.

[16] Bot é uma aplicação de *softwar*e para executar uma ação repetida.
[17] São virus para os quais não existem assinaturas no *software* de deteção.

(2) As ciberarmas.

(a) Os vírus fisicamente destrutivos.

Importa nesta fase evidenciar o aparecimento mais recente de vírus com elevada complexidade, mais difíceis de detetar e com a possibilidade de produzir danos muito para além dos danos informáticos, colocando em causa a segurança física das populações e infraestruturas das sociedades.

Em 2010, as centrifugadoras do programa de enriquecimento do Uranio no Irão, foram destruídas por um vírus, o *Stuxnet*[18]. "*A Symantec relatou o aparecimento de um novo e sofisticado vírus, designado por Stux net*" (Symantec, 2012). Este vírus foi introduzido nos sistemas informáticos de controlo das centrifugadoras, descontrolando-as posteriormente sem que os operadores se tivessem apercebido num primeiro momento, levando-as à sua autodestruição. Este vírus, embora já se conhecesse a sua existência, mostrou a sua eficácia pela primeira vez e marcou uma nova era de vírus, com a capacidade não só de contaminação dos sistemas informáticos, mas também de destruição física.

Dá-se assim o início de uma nova gama de vírus, não só com a capacidade de infetar os Sistemas de Informação (SI) mas também de realizar destruições físicas.

E outros vírus têm surgido. "*Depois de estudar o Stuxnet, o Duqu e o Flame, podemos afirmar com grau considerável de certeza que o Gauss veio da mesma 'fábrica' ou 'fábricas'. Todos esses kits de ataque representam esforços nacionais sofisticados de espionagem cibernética e de guerra cibernética patrocinados por Estados", afirmou a empresa de segurança Kaspersky sobre a ameaça."*(Terra, 2012).

(b) Nova tipologia de ciberataques.

Concorrentemente surgem novas tipologias de ataques a infraestruturas nacionais, que de forma coordenada e organizada, produzem também danos físicos. Consideremos as seguintes situações: um ataque a um sistema informático que controla o sistema de bombeamento e abertura/fecho de válvulas de um gasoduto, efetuado de forma a descontrolar o fluxo de combustível e destruir este meio; um cenário resultante de um ataque informático ao sistema de controlo dos sensores de posição, num metro em andamento, com o intuito de os descontrolar e causar um incidente final e de consequências desastrosas. Estes são alguns dos exemplos, que muito para além da ficção,

[18] Ver Anexo B: Ficha técnica do vírus Stuxnet 0.5:The Missing Link

são já fonte de preocupação internacional, da qual o cibercrime tem conhecimento e consciência e que mostram o potencial para uma nova ameaça, que no extremo poderá afetar a segurança e paz social ou mesmo a soberania de um País.

Estamos perante cenários em que as FFAA, no extremo poderão ter que intervir, atuando com os seus meios cibernéticos de carácter ofensivo ou mesmo convencionais cinéticos, caso não houvesse outro modo de os parar.

(3) Estados ciberarmados.

Estamos assim num momento em que os estados tomam consciência da capacidade letal dos novos vírus destrutivos e do potencial das novas ameaças nas redes digitais.

O ciberespaço corresponde a uma nova realidade estratégica, transversal às que já existiam, associadas à terra, mar, ar e espaço, criadas pelo homem e com características e problemas próprios.

Igualmente, surge a tomada de consciência da importância da superioridade da informação, vital para a vantagem competitiva das organizações e dos estados e na qual os militares têm um papel fundamental. Assim, em operações militares "*Quanto mais hábil um exército for na aquisição e gestão da informação de determinado contexto tático-estratégico dum conflito em que esteja empenhado, maior será a sua capacidade de minimizar as suas fraquezas e por outro lado, maior será a sua capacidade de identificar as vulnerabilidades do inimigo e potenciar o seu aparelho e força militar contra ele*" (Santos, 2008,p.99). A capacidade em obter dados vitais, ou em negar a sua cedência, utilizando a internet, é o contexto para uma nova forma de conflito entre os estados e uma razão para que através dos seus militares intervenham e desenvolvam competências para atingir aquela superioridade. Está em causa não só a elevada aplicabilidade ao ambiente operacional militar, conduzido numa dimensão digital, mas também a tomada de consciência de que as FFAA têm um papel vital na defesa das infraestruturas críticas nacionais, por um lado, e por outro o reconhecimento de que são um dos atores fundamentais para a construção da superioridade da informação a nível nacional.

Surgem desta maneira, nos últimos anos, a constituição de unidades de cibercomandos, com elevado número de efetivos e altamente especializados, tal como o *Cyber Command* (CYBERCOM) dos EUA com a missão de " *conduzir operações militares no ciberespaço em todo o espetro da ameaça*"(STRATCOM, 2010).

Simultaneamente, mais de trinta países nesta data já publicitaram unidades do mesmo tipo.

Adivinha-se, neste contexto, uma nova razão para o estabelecimento de novas relações de competição e conflitualidade entre estados e as suas organizações.

b. As capacidades de resposta aos ataques informáticos.

(1) A segurança informática nas organizações.

Tradicionalmente, as empresas e organizações com redes informáticas, conjugam normas e procedimentos de segurança com sistemas de proteção periféricos como *firewalls*[19], *intrusion detection system*[20], antivirus, que no passado revelaram alguma eficácia, mas face à complexidade das ciberameaças, têm-se revelado insuficientes.

Dentro desta linha tem tido grande aceitação o modelo de defesa em profundidade aplicado à segurança dos SI. Neste modelo de segurança da informação, utilizam-se várias camadas de proteção para os dados. O acesso direto a estas por um utilizador qualquer ou um sistema, só é possível, após terem sido reconhecidos nas camadas exteriores, em que estão embebidas regras de proteção e acessos, políticas de segurança, processos de negócio, recuperação de dados e continuidade de funcionamento, conjugados com análises de risco em todas as fases dos processos.

A segurança periférica continua a ser imprescindível, mas tem sido complementada com novos meios tecnológicos, conceptuais e organizacionais, que permitem uma nova abordagem.

Tecnologicamente, "*Os modelos para sistemas de defesa modernos apoiam-se nos sistemas de sistemas (Systems of Systems (SoS)), tirando partido do comportamento coletivo oferecem vantagens relativamente aos que atuam de forma individual. Estes sistemas podem ser regulados pelas mais variadas entidades e uma vez que possuem capacidades C2, é necessário garantir que os seus utilizadores obtêm a consciência situacional necessária ao ciberespaço*"[21] (Sousa, 2011).

Em termos organizacionais têm-se constituído os *Computer Emergency Response Team* (CERT), como a forma plausível de manter a continuidade de negócio das organizações e no limite dos estados.

[19] Dispositivo na forma de *software* e *hardware* que aplica uma política de segurança.
[20] Sistema de deteção de intrusões em uma rede, quando está tendo acessos não autorizados.
[21] O *Cyber Command, Control and Information Operations System* (C3IOS), só a título de exemplo, permite as mais variadas configurações, que melhor se ajustem de uma forma personalizada a um determinado ambiente e/ou incidente. Baseado em tecnologias distributivas, recorre a células virtuais, agentes móveis, reconfiguração dinâmica e endereços de *Internet Protocol* (IP) *hopping(alteram-se periodicamente com base num algoritmo)*, colaboração pró-ativa e antecipatória, que se traduz num sistema extremamente flexível e cooperativo.

(2) Os Computer Emergency Response Team (CERT).

Os estados e as organizações, como forma de melhorar a sua reação às ciberameaças, têm desenvolvido as suas Capacidades de Resposta a Incidentes de Segurança Informáticos (CRISI) constituídos por equipas de resposta imediata, em alguns casos com a designação genérica de CERT, que se têm revelado como uma forma mais eficaz de combater os ciberataques. Existem várias abreviaturas para o mesmo tipo de equipa e com capacidades mais ou menos semelhantes como *Computer Security Incident Response Team* (CSIRT), os *Incident Response Team* (IRT), as *Computer Incident Response Team* (CIRT) ou *Security Response Team* (SERT). O termo CERT ainda que esteja muito difundido, como está bastante ligado a uma equipa, tem sido substituído pelo termo CRISI.

O conceito CERT foi pioneiro em 1988 na Carnegie Mellon University, nos Estados Unidos. Na altura os seus investigadores concluíram que um número crescente de intrusões de rede, exigia uma equipa de resposta de emergência centralizada, para lidar diretamente com ameaças em tempo real. Estas equipas são constituídas por ciberespecialistas e detêm meios que lhes permitem monitorizar a internet ou uma rede de dados específica e reagir a um ciberataque ou uma ameaça informática, em coordenação com outros CERT.

No desenvolvimento desta capacidade, estes centros tem-se constituído como autênticos provedores de serviços de segurança, incluindo não só os serviços de prevenção, tais como alertas e avisos de segurança, mas também treino de equipas, serviços de gerenciamento de acidentes informáticos, recuperação de desastres, continuidade do negócio ou avaliação de produtos informáticos, estabelecendo acordos que lhes permitem adquirir conhecimentos e troca de informação técnica, de forma a responder com maior eficácia.

Os CERT podem ser agrupados por vários setores: académicos, comerciais, governamentais, empresariais, militares, entre outros.

Os CERT militares, estão também associados às infraestruturas críticas e ao Centro Nacional de Cibersegurança (CNC)[22], com o qual deverão estar profundamente coordenados de forma a maximizarem a capacidade de resposta, em situações mais graves.

Hoje, existem mais de 250 CERTs operacionais em todo o mundo, embora alguns membros da NATO ainda não os tenham constituído.

[22] Confirmaremos mais à frente neste trabalho esta necessidade.

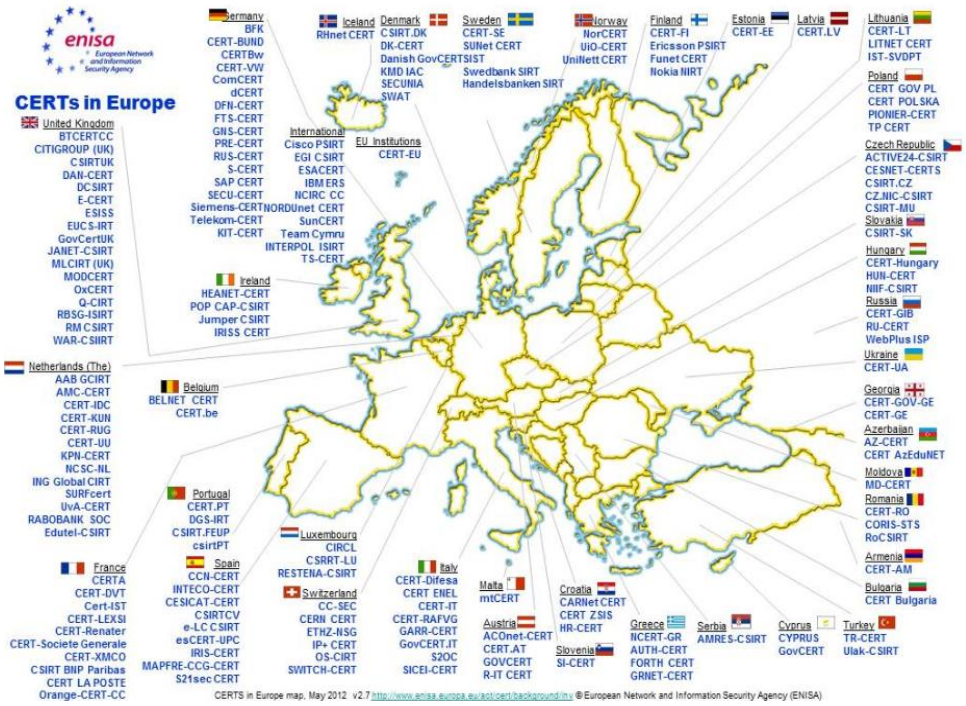


Figura nº3: CERT na Europa

Fonte: (ENISA, 2012)

(3) A ciberguerra.

Os conflitos processam-se atualmente em ambientes assimétricos, de forma irregular, sem frentes definidas, sem fronteiras claras e com objetivos fluidos. O ciberespaço é um ambiente com características tipicamente assimétricas, palco de uma nova era de conflitos não convencionais entre estados.

A ciberguerra[23] materializa todo o conjunto de ações de defesa, prospeção e ataque contra infraestruturas de informações e redes de computador existentes em todos os meios militares de comando e controlo (C2), utilizados em ambiente operacional, conduzido necessariamente numa dimensão digital e designados por *Computer Network Operations* (CNO).

O emprego operacional dos meios de ciberdefesa das FFAA tem como referência a doutrina NATO. Assim de acordo com a Publicação Conjunta da NATO AJP 3-10 (Operações de Informações), as CNO representam um dos recursos principais das Operações de Informação (IO) e por sua vez, subdividem-se em três domínios:

[23] O termo ciberguerra tem sido substituído por ciberdefesa, sendo adotado pelo autor neste trabalho.

-*Computer Network Defense* (CND): Ações executadas para proteger, monitorizar, analisar, detetar e reagir a atividade não autorizada dentro dos sistemas de informação e redes de computadores;

-*Computer Network Exploitation* (CNE): A capacidade de executar operações de recolha de informações conduzidas através da utilização da rede de computadores, para reunir dados dos alvos adversários, dos seus sistemas de informação ou das suas redes de computadores;

-*Computer Network Attack (CNA):* Ações executadas através da utilização de redes de computadores para romper, negar, degradar, ou destruir a informação residente nos computadores e redes de dados adversários.

As CNE poderão ser executadas com a finalidade de obter informações e o conhecimento atualizado do ambiente digital que nos rodeia, numa área de operações militares, para ser usado mais tarde em proveito de uma ação ofensiva.

As CNA poderão ser conjugadas com o início de operações militares e posteriormente atacando alvos considerados remuneradores. Poderão ainda ser utilizados como forma de nos defendermos, impedindo que um ataque opositor se realize.

Não é do âmbito deste trabalho analisar o emprego dos meios de ciberdefesa em operações militares. Pretende-se no entanto, dar uma ideia do contributo e qual o contexto, em que os meios de ciberdefesa poderão ser utilizados em tempo de paz, com o objetivo de repor a soberania nacional.

Em termos nacionais, o emprego das FFAA está previsto, conjugando o art.º 273º da CRP em que *"A defesa nacional tem por objetivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações, contra qualquer agressão ou ameaça externas"*, com o *art.º275º "Às Forças Armadas incube a defesa militar da República"*.

Internacionalmente o emprego dos meios de ciberdefesa das FFAA "*É enquadrado pelo Direito Internacional Humanitário (DIH), ou como também é conhecido Lei dos Conflitos Armados (LCA). O DIH, define o comportamento e as responsabilidades das nações beligerantes, nações neutras e indivíduos envolvidos na guerra, em relação uns aos outros e em relação a civis. A lei tem duas partes: lei da gestão de conflitos (jus ad bellum) e o direito da guerra (jus in bello)"* (Sousa, 2011).

Por outro lado, um dos desafios do ciberespaço é o de definir e detetar se um ato hostil escalou tal ordem, que justifique o uso da força. Vários processos poderão ser utilizados para esse fim. "*A Análise de Schmitt*[24]*, pode ser aplicada para caracterizar o tipo e nível das ameaças, de acordo com o espectro das suas consequências induzidas e identificar a necessidade do uso da força*" (Sousa, 2011).

Assim, a utilização dos meios de ciberdefesa das FFAA, pressupõe um enquadramento legal que autorize os meios de ataque por um lado, e por outro, a intensidade do impacto gerado pelo ciberataque hostil, que justifique uma resposta do tipo ofensiva. Em situações em que as infraestruturas críticas nacionais ou organismos do estado possam ser colocados fora de funcionamento após ataques cibernéticos e sendo posta em causa a soberania nacional, só os recursos de ciberdefesa, em coordenação com os restantes meios existentes na FFAA do país, têm enquadramento legal e a capacidade para serem empregues de forma a repor a paz e a soberania nacional.

Repare-se que só as FFAA podem executar de uma forma legal, as CNO[25] como forma de defesa, aliás como qualquer outro emprego dos meios militares.

É neste contexto que se considera que os meios de ciberdefesa das FFAA serão a garantia final, na liberdade de utilização do ciberespaço, na área de interesse do país.

c. A proteção das infraestruturas críticas nacionais.

Os estados modernos, são constituídos por um elevado número de infraestruturas transversais a todo o território nacional, com grande incorporação tecnológica para o seu funcionamento e operação. Algumas destas são consideradas infraestruturas críticas e estão definidos genericamente pelo Dec Lei 62/2011 de 9 de Maio como "*A componente, sistema ou parte deste situado em território nacional, que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções*". Estão em causa infraestruturas, que utilizando sistemas de informações e redes de telecomunicações no seu comando e controlo, poderão ser afetadas por ciberataques, podendo ficar inoperacionalizadas colocando em causa o

[24] A análise de Schmitt avalia um acidente em sete critérios (severidade, imediatismo, clareza, invasividade, mensurabilidade, legitimidade presumida e responsabilidade) para determinar o grau de gravidade de uma ciberameaça.
[25] "*A capacidade ciber ofensiva, no entanto, inclui atores fora do controle direto do governo. Por exemplo, os hackers independentes, criminosos e flash mobs podem ser usados para atacar um alvo por procuração, ampliando as capacidades cibernéticas ofensivas de um Estado-nação*"(Melo,2010).

funcionamento regular do país ou mesmo, no extremo, a sua soberania. Incluem-se nestas infraestruturas, entre outras, os sistemas de energia elétrica nacional, as redes de telecomunicações, os transportes, o Serviço Nacional de Saúde (SNS), o sistema bancário e os organismos do estado.

Será da responsabilidade dos dirigentes destes organismos, em coordenação com as entidades nacionais de segurança e defesa contra ciberataques, desenvolver medidas para contrariar as ameaças cibernéticas. Além das medidas de segurança periférica dos sistemas de informação e comunicações, destaca-se também a criação de CERT, associados a estas infraestruturas criticas, que terão como objetivo desenvolver as ações e a coordenação necessária com o centro nacional de cibersegurança, no sentido de mitigar os efeitos dos ataques informáticos.

É desejável assim, que os responsáveis políticos e as classes dirigentes tomem consciência, que com relativa facilidade o ciberespaço e a internet, poderão ser utilizados por indivíduos ou grupos criminosos, colocando em causa o funcionamento destas infraestruturas e a sua segurança, sendo desejável que se desenvolvam procedimentos e mecanismos de partilha, que evitem tais situações.

É também nesta situações extremas, tal como referido anteriormente, em que a soberania e a regularidade de funcionamento de um estado estejam em causa, que as capacidades de ciberdefesa dos militares poderão ser solicitadas e colocadas de forma a contrariarem os ciberataques, já que só eles são detentores de tais capacidades e, que em situações extremas, a CRP lhes permite deter e utilizar.

d. Cibersegurança vs ciberdefesa.

Percebe-se nesta fase do trabalho, a existência de dois domínios, que não estando definidos doutrinariamente, interessa diferenciar: a cibersegurança e a ciberdefesa.

A ciberdefesa corresponde, tal como já se viu, à deteção, análise, monitorização, proteção, recolha de informações e às ações para romper, negar, degradar, ou destruir a informação residente nos computadores e redes de dados adversários. Estas ações podem realizar-se em ambiente operacional de guerra ou em resposta às ciberameaças que coloquem em causa a soberania e a segurança nacional e que são primariamente da responsabilidade das FFAA.

A cibersegurança corresponde a um conjunto de medidas em que se conjugam normas e procedimentos de segurança com sistemas de proteção periféricos tais como *firewalls*, IDS, antivirus, associados a CERT, para enfrentar as ameaças e ataques

realizados no ciberespaço. De uma forma geral cabe aos organismos e empresas desenvolver as ações necessárias para a sua proteção. No caso especifico em que possam ser tipificadas em cibercrime, ciberativismo[26], ciberespionagem ou ciberterrorismo, são da responsabilidade primária, das forças de segurança e do Serviço de Informações de Segurança.

Em situações de ameaça vindas do ciberespaço que coloquem em causa infraestruturas críticas num grau tão elevado que seja posta em causa a soberania nacional, tal como está definido na CRP, será da responsabilidade das FFAA aplicar a sua capacidade de ciberdefesa. Só nesta situação, poderão utilizar a sua capacidade de desenvolver as CNO como medida de defesa, eventualmente conjugados com meios cinéticos.

As FFAA podem assim participar e garantir na defesa e segurança do ciberespaço no domínio nacional. Intrinsecamente deverá ser sempre considerada a existência de uma área de cibersegurança global, sob a qual coexistam em paridade, complementando-se as áreas da cibersegurança e da ciberdefesa.

e. As FFAA nacionais na resposta aos incidentes informáticos.

Para efetivar o comando e controlo (C2) e a gestão das suas unidades e órgãos, as FFAA utilizam sistemas de comunicações e de informações, suportados por doutrina e procedimentos de operação destes meios.

Comum aos três Ramos, a Rede Fixa de Comunicações Militares (RFCM), estende-se por todo o território nacional é constituída por um sistemas de feixes hertzianos, fibra ótica e equipamentos de transmissão de dados (servidores e routers), que constituem o *backbone*[27] nacional das FFAA.

Estas estruturas são mantidas e administradas pelo pessoal dos respetivos Ramos, em número reduzido e alguns em acumulação de funções. Alguns dos elementos têm cursos na área da segurança dos SI sendo suficientes para as necessidades de cibersegurança. No entanto são em número reduzido se considerarmos a exigência de núcleos de ciberdefesa. Não existem ainda elementos das FFAA a frequentar cursos no CCDOE em Tallin por exemplo. Existem elementos a participar em seminários nacionais e internacionais, assim como em fóruns da NATO;

[26] Ativismo desenvolvido no ciberespaço.
[27] O *backbone* é neste caso a estrutura principal da rede de dados das FFAA.

As unidades e órgãos militares que se encontram dispersas por todo o território nacional tem meios e redes individuais, que se interligam à rede nacional, permitindo serviços de voz, dados, *mails* e partilha de dados de uma forma geral.

Quando necessário, caso a tipologia do meio o exija ou em forças militares presentes fora do território nacional, utilizam-se meios de comunicação rádio ou satélite, para manter a continuidade dos sistemas de C2.

As redes estabelecidas, têm vários níveis de segurança conforme o grau de classificação da informação que se pretende transmitir. As redes com segurança mais elevadas são isoladas de todas as outras e tem regras muito apertadas de acesso, exploração e funcionamento. Nas redes de seguranças mais baixas são estabelecidas regras e procedimentos específicos, os dados são encriptados e os sistemas de filtragem exigentes, de forma a evitar quebras de segurança. Sendo mais abertas aos utilizadores, é permitido o acesso à internet, sendo este, controlado e filtrado por *software* e *hardware* específicos.

As redes das unidades dos Ramos em operações, são interligadas a estas últimas, de forma a maximizar as operações centradas em rede, dando essencialmente prioridade à disponibilidade da informação.

Os Ramos implementam as suas redes, aplicando regras e sistemas de segurança, com o objetivo de se protegerem das ciberameaças, sem contudo perderem a operacionalidade e os requisitos de segurança necessários. Mas quais são as capacidades desenvolvidas e implementadas pelas FFAA para a proteção das suas redes?

(1) O Exército.

Este ramo possui uma estrutura de Sistemas de Informação e de Comunicações Operacional (SIC-O), com cobertura em todo o território nacional, e um Sistema de Informação e Comunicações Tático (SIC-T), que permite desenvolver o C2 em todas as suas Unidades, Estabelecimentos e Órgãos (U/E/O) e unidades táticas.

No sentido de obter uma capacidade eficaz no domínio da guerra da informação, desenvolveu uma Capacidade de Resposta a Incidentes nos Sistemas Informáticos (CRISI) em concordância com a diretiva do Estado Maior do Exército (EME), (EME, 2008) e o PEMGFA CSI301 (EMGFA, 2008). Assim implementou uma estrutura constituída por antivírus, *firewall*, IDS, NAC[28] e um sistema de correlação de eventos, em toda a sua estrutura SIC-O e SIC-T que associados a um conjunto de políticas de segurança muito

[28] Controle de acesso á rede.

restritivas, lhe confere uma capacidade de segurança em profundidade contra ciberataques e ameaças informáticas.

Concorrentemente, desenvolveu uma capacidade tática, *Computer Incident Response Capability* (CIRC), com a missão de apoiar a vertente ofensiva no Ciberespaço, sendo capaz de desenvolver todo o tipo de CNO, nomeadamente, efetuar intrusões, tendo em vista afetar os princípios básicos de segurança (confidencialidade, integridade e disponibilidade) nos sistemas de informação e comunicações adversárias, conseguindo desta forma implementar uma capacidade única nas FFAA de ciberdefesa. "*O Exército, em devido tempo, organizou-se por necessidade própria. Como requisito ao nível operacional e tático...tínhamos de garantir a proteção da nossa informação, de a proteger, de ter alguma capacidade de a extrair e numa situação real, porque a situação não é sempre defensiva, ter inclusive alguma capacidade de ataque*"(Matias, 2012).

Este módulo, está sedeado no Regimento de Transmissões (RTm) e em termos operacionais articula-se sob o Comando do Batalhão de Transmissões, da Escola Prática de Transmissões (EPT). Operacionalmente, tem sido utilizado em exercícios para detetar vulnerabilidades nos sistemas de informação táticos do Exército e ajudar a desenvolver procedimentos e mecanismos para os corrigir.

(2) A Marinha.

Os Sistemas de Informação e Comunicações Automatizada (SICA) armazenam, processam e transmitem informação de cariz operacional e administrativo, necessário ao comando e controlo da Marinha e são devidamente protegidas.

A proteção dos SICA requer a implementação e gestão de políticas de segurança adequadas, mas também uma estrutura capaz de monitorizar, identificar, alertar, responder e recuperar, na eventualidade de uma quebra de segurança relacionada com as falhas de confidencialidade, integridade, disponibilidade, autenticação e não-repúdio da informação.

Para este fim, a Marinha implementou uma CRISI, que permite responder de forma concertada a incidentes de segurança da informação, relacionados com atividades de *software* malicioso, negação de serviços, ou outras ameaças ou vulnerabilidades e minimizar o seu impacto nos SICA, garantindo uma resposta adequada. A edificação da CRISI surgiu da necessidade de se concretizar o exposto nas diretivas internas e nas recomendações NATO e UE e encontra-se definido na PCA 16 da Marinha[29](EMA, 2012).

[29] Publicação de Comunicações da Armada, *Conceito de implementação da capacidade de resposta a incidentes de segurança da informação na Marinha*.

Esta estrutura de cibersegurança facilita a partilha de estratégias de resposta e a divulgação de alertas relativos a potenciais problemas.

De acordo com o PCA 16 da Marinha, a CRISI visa igualmente aprontar um grupo com valências na área da segurança dos sistemas de informação e comunicações, dedicado a apoiar a Marinha, na prevenção e mitigação de incidentes de segurança da informação, bem como na proteção dos recursos críticos. Possui a capacidade de isolar, rápida e atempadamente, um incidente de segurança, de forma a evitar a sua proliferação à restante estrutura e SICA da Marinha. É capaz de gerir eficazmente a resposta aos incidentes informáticos de forma centralizada e recuperar automáticamente; tem capacidade de cooperação em matéria de resposta a incidentes de segurança da informação com os outros Ramos das Forças Armadas e outras organizações da mesma natureza.

Ainda segundo o PCA 16 da Marinha, os serviços disponibilizados pela CRISI são organizados nas seguintes áreas:

- Serviços reativos, constituídos por tratamento de alertas e avisos, gestão de incidentes, análise, coordenação e resposta a incidentes informáticos.
- Serviços pró-ativos, constituídos por análise, gestão e mitigação de vulnerabilidades; divulgação de informação aos utilizadores; acompanhamento do conhecimento técnico nesta área; colaboração em auditorias ou avaliações de segurança da informação; serviços de monitorização e deteção de intrusão; divulgação de informações relacionadas com a segurança da informação.
- Serviços de gestão de segurança e de qualidade de serviço, constituído por: colaboração em análises de risco; contribuição para a implementação de planos de prevenção, reposição, contingência e emergência; emissão de pareceres no âmbito da segurança da informação; promoção de seminários, treino, formação ou outras formas de sensibilização; contribuição para a definição de requisitos operacionais de soluções de segurança.

A estrutura do CRISI de acordo com o PCA 16, está subdividida em três níveis:

Nível 1 – Entidade de Coordenação da CRISI, que se situa no Estado-Maior da Armada (EMA) e que funciona como entidade de coordenação de resposta a incidentes de segurança da informação, assessoria jurídica e ligação com entidades externas.

Nível 2 – Grupo de Resposta a Incidentes de Segurança da Informação onde se encontram as Áreas das Tecnologias da Informação e Operacional, que disponibilizam

apoio na deteção, análise, resposta e recuperação a incidentes de segurança da informação, providenciando igualmente o apoio técnico às Autoridades Operacionais dos SICA, no que respeita à deteção de intrusão e prevenção de software malicioso.

Nível 3 – Entidades da Organização de Segurança dos SICA, às quais corresponde a respetiva organização e segurança e o relato de qualquer atividade suspeita que ocorra na sua área de competência, através da sua estrutura SICA.

(3) A Força Aérea.

A FA possui uma defesa em perímetro, às suas infraestruturas de CSI, utilizado para tal *firewall*, IDS, NAC e antivírus não possuindo no entanto, qualquer sistema de correlação de eventos que lhe permita determinar qualquer ataque informático aos seus sistemas. Efetua back-up periódicos, que lhes permite efetuar um ação de *recovery disaster* limitado.

Faz parte da rede de CERT-pt da Fundação Cientifica de Computação Nacional (FCCN) e encontra-se representada no CRISI do EMGFA.

Participa em vários fóruns a nível nacional sobre cibersegurança.

Possui um documento aprovado neste domínio, RFA 390-6, Politica de ciberdefesa da Força Aérea, desde Fevereiro de 2011.

Em termos organizacionais a resposta a incidentes informáticos está organizada em três níveis:

1ºnivel-EMFA/DivCSI, onde se desenvolve a política de ciberdefesa.

2ºnivel-CLAFA/DCSI, na qual se encontra o grupo de resposta a incidentes informáticos.

3ºnivel-Centros de informática das unidades, aonde é efetuada a coordenação com os Oficiais de Segurança Local dos SIC (OSSIC) e os Administradores Locais dos SIC (ALSIC), de acordo com os procedimentos estabelecidos pela DCSI.

(4) O Estado-Maior-General das Forças Armadas.

Na área da ciberdefesa, é da sua responsabilidade promover a implementação de uma política conjunta de segurança da informação, de forma a garantir a autonomia, sobrevivência e interoperabilidade dos sistemas das FFAA.

Através da sua publicação (EMGFA, 2008), estabeleceu-se a estrutura orgânica, normas e procedimentos, para garantir a capacidade de resposta a incidentes de segurança informática das FFAA.

O CRISI do EMGFA, embora com recursos limitados, encontra-se operacional nesta data e desenvolve a sua atividade nas áreas de segurança informática, relacionadas com *software* malicioso, atividades de utilizadores não autorizados, negação de serviços, ou outras ameaças/vulnerabilidades inerentes aos SIC. Esta capacidade utiliza de forma coordenada as valências existentes nos Ramos das FFAA e no EMGFA, disponibilizando serviços reativos, pró-ativos e de gestão de segurança e qualidade de serviço.

Para a gestão e tratamento de incidentes de segurança informática dispõe ainda de um sistema de registo de incidentes e de um portal CRISI. A estrutura da CRISI - assente no princípio da eficiência - procura obter uma resposta coordenada dos recursos existentes, em três níveis de atuação e coordenação: o Centro de Coordenação da CRISI, o Grupo de Resposta a Incidentes de Segurança Informática (GRISI) e, um ultimo, composto pelas Autoridades de Segurança dos SIC.

f. Síntese conclusiva.

As sociedades dependem cada vez mais do ciberespaço, aumentando-lhes as oportunidades de desenvolvimento e interação à escala global. Paralelamente, torna-se também abrigo de novos atores, caraterizados e tipificados ao longo do trabalho que, de forma ilegal, tiram partido desta nova dimensão, constituindo um novo perigo para as organizações e os estados.

Evidenciaram-se as metodologias e as estratégias na segurança dos SIC, melhorando a defesa em profundidade e a criação de CERT, para dar resposta às ameaças cibernéticas.

As FFAA, inseridas num mundo digital, como órgão de defesa do estado, também desenvolveram, para além da sua capacidade de cibersegurança, as competências para efetuarem ciberdefesa. Têm assim um papel fundamental, não só na segurança da sua organização, mas também na continuidade da soberania dos estados, disponibilizando quando necessário as suas capacidades na proteção das infraestruturas críticas e dando continuidade ao funcionamento dos organismos do estado.

No desenvolvimento de capacidades contra os ciberataques, verificamos de comum aos Ramos e ao EMGFA os seguintes aspetos:

- Implementação de medidas de segurança em profundidade dos SIC que configuram uma capacidade de cibersegurança nas FFAA;
- Existência de documentação enquadrante do funcionamento, organização e resposta aos incidentes informáticos;

● Pessoal dedicado à área da segurança dos SIC, embora em número reduzido e alguns em acumulação de funções;

● Alguns dos elementos têm cursos na área da segurança dos SI, mas muito reduzida para a exigência de núcleos de cibersegurança e/ou ciberdefesa. Não existem ainda elementos das FFAA a frequentar cursos no CCDOE em Tallin por exemplo;

● Existem elementos a participar em seminários nacionais e internacionais, assim como em fóruns da NATO;

● Aquisição de equipamentos e sistemas aplicacionais orientados para a cibersegurança;

● Participação em exercícios de ciberdefesa e cibersegurança, nacionais, da NATO e da UE;

● O CRISIS do EMGFA, efetua reuniões periódicas para coordenação e troca de informação técnica com o CERT.pt;

● Organização em três níveis; doutrinário, operacional e táctico/utilizador das suas estruturas de cibersegurança/ciberdefesa e com diferentes graus de desenvolvimento;

● O Exército é o único ramo que possui atualmente a capacidade de ciberdefesa ou seja, a capacidade de efetuar CNO em todo o espectro das operações no ciberespaço.

Assim perante a QD1-"*Qual é a capacidades de ciberdefesa já desenvolvida pelas FFAA?"*, conclui-se que os Ramos e o EMGFA, têm efetuado um esforço de investimento nos seus meios, em pessoal, infraestruturas e desenvolvido uma regulamentação enquadrante, o que lhes confere uma capacidade de cibersegurança de forma geral. Em particular, o Exército desenvolveu uma capacidade de ciberdefesa.

Apesar desta evolução, consideramos que se encontram em diferentes estádios de consolidação e maturação da sua capacidade de proteção contra as ameaças no ciberespaço, confirmando-se a H1-"*As FFAA dispõem de uma capacidade limitada na luta contra os ciberataques"*.

2. A ciberdefesa cooperativa atualmente desenvolvida pelas FFAA.

a. A Estratégia Nacional de Cibersegurança (ENC).

A ENC deverá ser entendida no domínio de uma Estratégia Nacional de Segurança da Informação (ENSI), e esta, integrada numa Estratégia Nacional de Segurança e Defesa. Em Portugal, de acordo com a Resolução do Conselho de Ministros (RCM) nº12 (Governo, 2012), até ao final de 2012, deveria ter sido definida e implementada uma ENSI, definindo o responsável pela implementação da segurança de informação no país, a sua estrutura, os serviços que seriam fornecidos e, por último, quem seria o responsável por medir e gerir o risco e auditar a segurança da informação. Tal não aconteceu, por diversas razões que não cabe aqui abordar.

Apesar desta indefinição e tal como é considerado por alguns autores, "*A Estratégia Nacional de Cibersegurança, pode ser definida como o conjunto integrado de iniciativas (de natureza orgânica, operacional e genética), destinados a potenciar a livre, utilização do ciberespaço e garantir a sua segurança, promovendo a proteção da Infraestrutura de Informação Critica Nacional contra eventuais ciberataques, de âmbito nacional ou internacional que, pelo seu carácter disruptivo, afetem a sociedade portuguesa e a defesa dos Interesses Nacionais*" (Nunes, 2012a, 115).

Complementarmente, de acordo com o Gabinete Nacional de Segurança (GNS), existe a necessidade do país levantar uma Estrutura Nacional de Cibersegurança (ENC), composta por uma capacidade de nível essencialmente operacional, um Centro Nacional de Cibersegurança e uma capacidade de nível estratégico, um Conselho de Cibersegurança, capaz de garantir uma eficaz gestão de crises. Esta ENC seria capaz de coordenar a resposta operacional a ciberataques, desenvolver sinergias nacionais e potenciar a cooperação internacional neste domínio.

É em consonância com este desígnio, que se encontra em fase de definição e edificação a nível nacional, que as FFAA estão já a desenvolver as estratégias genética, estrutural e operacional, na implementação das suas estruturas de ciberdefesa, nomeadamente aquelas de aspeto cooperativo e de partilha de informação.

Torna-se claro, num primeiro passo, que só com uma estratégia de partilha, concertada entre todos os intervenientes nacionais, que edificam as suas capacidades contra os ciberataques ou que já se encontram em fase de operacionalização das mesmas, será possível atingir alguma eficácia nesta área.

b. A capacidade de resposta aos ciberataques a nível nacional.

(1) O Centro Nacional de Cibersegurança (CNC).

Em Portugal, em consonância com a RCM nº12 de 2012 e as diretivas da UE, deveria ter sido criado um CNC[30] com poder institucional, até ao final de 2012.

Tal ainda não aconteceu, tendo o governo através da RCM nº112/2012 de 31 de dezembro de 2012 aprovado a constituição de um outro organismo, eventualmente equivalente ao CNC.

O CNC em coordenação com os CERT nacionais[31], iriam constituir a capacidade técnica e operacional de resposta nacional a incidentes informáticos. Assumiria também o papel de representante nacional nesta área, cumprindo as normas europeias que previam a criação de uma unidade de resposta em Portugal. Constituiria assim a entidade mais preponderante no desenvolvimento e coordenação das áreas de cooperação nacional e internacional na cibersegurança e ciberdefesa.

O que é facto é que na ausência do CNC, até esta data, o CERT.pt da FCCN tem sido a entidade que tem efetuado o papel de coordenador nacional. É a entidade nacional, reconhecida pelos seus pares internacionalmente e que continua em funcionamento até esta data.

(2) O CERT.pt

O CERT.pt foi criado e é gerido por uma fundação, a FCCN, com o objetivo de responder a incidentes de segurança informática no contexto da comunidade utilizadora da Rede Ciência, Tecnologia e Sociedade (RCTS). Presta apoio a utilizadores de sistemas informáticos na resolução de incidentes de segurança, difundindo as boas práticas de segurança, aconselhando procedimentos, analisando factos e coordenando ações com as entidades envolvidas. Reúne e dissemina informação relacionada com novas vulnerabilidades de segurança e produz recomendações referentes a potenciais riscos de segurança e atividades maliciosas em curso, no sentido de formar uma consciência de segurança junto dos utilizadores de sistemas informáticos. Difunde indicadores e informação estatística nacional sobre incidentes de segurança. Promove a criação de novos CSIRT em Portugal e a cooperação entre estes.

Legalmente, não pode ser reconhecido como representante do Estado Português tanto a nível nacional como a nível internacional – ainda que, na prática, empresas e

[30] Este deveria integrar o *European Information Sharing and Alert System* (EISAS).
[31] Nos quais estaria incluído o CERT das FFAA.

ministérios portugueses, e as organizações internacionais como a própria Agência da Rede Europeia de Segurança e Informação (ENISA) considerem que o CERT.pt é o interlocutor a que devem recorrer sempre que se trata de analisar possíveis ameaças e vulnerabilidades de cibersegurança. Ressalta-se no entanto que em situações mais complexas, como ciberataques de grau mais elevado, em conflitos de interesses entre instituições ou em procedimentos errados, os responsáveis pelo CERT.pt, na ausência de um diploma legal que lhes confira poder para assumir o controlo das operações, tem um grau de ação muito reduzido. De relevante ainda, o facto de a FCCN encontrar-se em extinção, transitando as suas funções para a Fundação para a Ciência e Tecnologia (FCT), sendo incerto o destino do CERT.pt.

Tem nesta data, estabelecido um conjunto de protocolos com CERTs nacionais e internacionais, entre os quais o do EMGFA.

c. A cooperação entre as FFAA e os CERTs nacionais.

(1) A partilha entre as FFAA.

Tal como previsto no PEMGFA CSI 301, o EMGFA implementou um Centro de Resposta a Incidentes nos Sistemas Informáticos (CRISI) com a seguinte estrutura:

● O Centro de Coordenação do CRISI (CC-CRISI) – No qual os Ramos têm representantes com responsabilidades na definição de políticas de segurança da informação e ciberdefesa e na coordenação das respostas aos incidentes de segurança informática. Este Centro assume a coordenação da resposta a incidentes sempre que o sistema afetado seja conjunto e proporciona, ainda, a discussão das políticas e procedimentos a implementar nos sistemas CSI dos Ramos e do EMGFA, de forma coordenada.

● O Grupo de Resposta a Incidentes de Segurança Informática (GRISI) composto por pessoal técnico, nomeado pelas respetivas Direções Técnicas dos Ramos, que é responsável por receber, analisar e responder a notificações e atividades relacionadas com incidentes de segurança em sistemas informáticos, bem como a sua recuperação. Reportam diretamente ao CC-CRISI.

O CRISI envolve ainda os elementos da organização de segurança das UEO dos Ramos e do EMGFA para tratamento e resposta a incidentes de segurança informática, os respetivos utilizadores, os meios de comunicações de relato e de registo de incidentes, bem como a coordenação da sua formação e consciencialização individual.

Existe assim uma ação concertada entre os Ramos e o EMGFA na partilha de informação técnica e resposta aos incidentes informáticos, em sintonia com as

determinações do PEMGFA 301. De referir ainda, que esta é uma capacidade conjunta que funciona com algumas limitações temporais, devido ao reduzido numero de pessoal diariamente envolvido nesta atividade.

Destaca-se ainda a realização do "Cyber Perseu", exercício nacional dinamizado pelo Exército, realizado em 2012, no qual foi testado o módulo tático CIRC do Exército e em que os restantes Ramos participaram como observadores.

(2) Áreas de partilha entre FFAA e as entidades exteriores.

O EMGFA estabeleceu um protoloco de cooperação com o CERT.pt da FCCN, no âmbito da resposta a incidentes informáticos e troca de informação técnica.

Efetua reuniões periódicas com a comunidade de CERT nacionais com o fim de partilhar informação técnica, conhecimento sobre novas ameaças e desenvolvimento de procedimentos e formas de evitar e resolver ameaças catalogadas.

Ainda no âmbito da cooperação e partilha de conhecimento, as FFAA têm participado em diversos exercícios nacionais e internacionais, de forma a desenvolver as suas competências e melhorar os procedimentos de resposta às ameaças informáticas.

Os militares dos Ramos participam também regularmente em seminários, conferencias, workshops, apresentações de novos produtos e reuniões técnicas nacionais e internacionais, estas ultimas principalmente na NATO.

d. As organizações internacionais.

(1) Agência Europeia para a Segurança das Redes e da Informação (ENISA).

É a entidade que apoia os Estados-Membros no intercâmbio de boas práticas no domínio da cibersegurança e apresenta recomendações sobre como desenvolver, aplicar e manter uma estratégia de cibersegurança. Tem ainda como função, apoiar as estratégias nacionais de cibersegurança e os planos nacionais de emergência. Organiza exercícios pan-europeus e internacionais sobre a proteção das infraestruturas críticas da informação, criando os respetivos cenários.

Tem ainda como objetivos: investir na investigação e no desenvolvimento em matéria de cibersegurança e de ciberdefesa, essenciais para a sua manutenção e evolução; sensibilizar e formar os cidadãos, base de qualquer estratégia global de cibersegurança; cooperar e coordenar dentro das instituições da EU e desenvolver uma estratégia global na UE em matéria de cibersegurança como condição prévia para o estabelecimento de uma cooperação internacional eficiente neste domínio exigida pela natureza transfronteiriça das ciberameaças.

Ainda de acordo com a ENISA, tendo em conta os valores e interesses estratégicos comuns entre a EU e a NATO, estas terão uma responsabilidade e uma capacidade especiais de abordar mais eficientemente, em estreita cooperação, os crescentes desafios no domínio da cibersegurança, através da procura de eventuais complementaridades, no respeito das suas responsabilidades, através da partilha a nível prático, no planeamento, na formação e nos equipamentos a escolher no contexto da cibersegurança e ciberdefesa.

Tendo por base as atividades complementares no domínio do desenvolvimento de capacidades de defesa com a NATO, a ENISA pretende esforçar-se com o objetivo de realizar um intercâmbio de experiências e de aprender a reforçar a resiliência dos sistemas da UE.

A ENISA desempenha assim um papel relevante em apoio à Comissão Europeia e ao desenvolvimento da cooperação entre os estados membros e organizações como a NATO e nos quais Portugal tem participado.

De relevar que, em consonância com o papel da ENISA, em 7 de fevereiro de 2013 a Comissão Europeia publicou uma estratégia em matéria de cibersegurança, assim como uma diretiva sobre segurança das redes e da informação, traduzindo a visão global da EU.

(2) A Organização do Tratado do Atlântico Norte.

Esta organização já compreendeu há longo tempo, a importância da utilização do ciberespaço.

Em 2008 foi criada a "Autoridade NATO para a Gestão da Defesa no Ciberespaço o *Cyber–Defence Management Authority* (CDMA)", com a missão de estabelecer ligações com as organizações nacionais que tratam da segurança no ciberespaço.

Apoiou a criação e o desenvolvimento do "*Cooperative Cyber Defence Centre of Excellence*" (CCD COE) em Tallinn na Estónia, em Maio de 2008, com recursos humanos, materiais e financeiros e providenciou a formação e treino, com o objetivo de melhorar as capacidades defensivas da NATO no Ciberespaço. Este centro consubstancia assim um esforço internacional visando a educação e o treino, a investigação e o desenvolvimento e a cooperação e a troca de informação entre as Nações NATO, incluindo outros países parceiros. Portugal já participou em seminários que decorreram em Tallin, mas não existem registos de qualquer formação para militares portugueses neste centro.

Foi também implementada uma Capacidade para Resposta a Incidentes de Computador, " *NATO Computer Incident Response Capability*" (NCIRC), composta por vários níveis de intervenção para permitir gerir os eventos no ciberespaço. Dispõe de

ligações diretas às estruturas nacionais (nas quais se insere Portugal e as suas FFAA), para enfrentar as ameaças e mitigar as vulnerabilidades de forma partilhada.

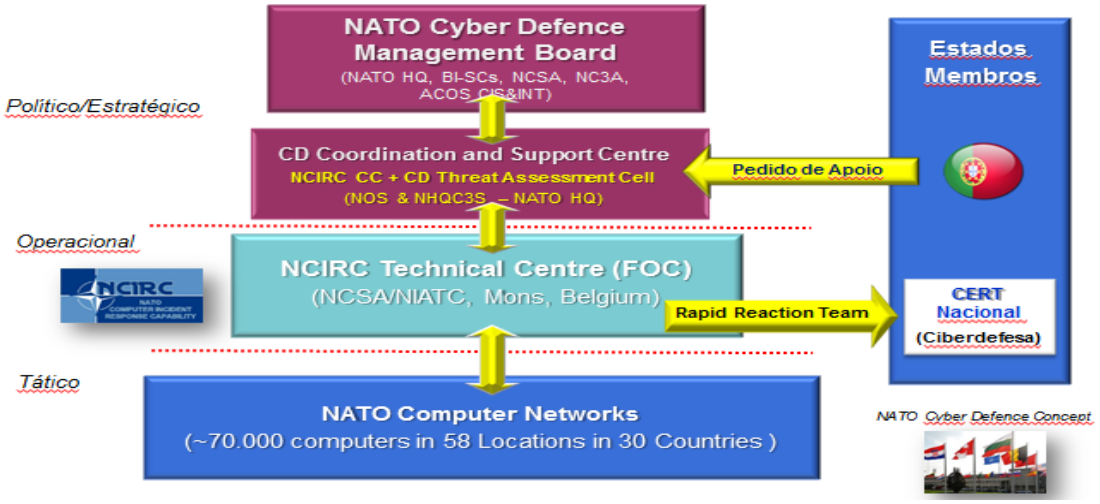


Figura nº4: Organização da NATO na ciberdefesa

Fonte: (Nunes, 2012b)

Esta vertente está em evolução e novos serviços foram-lhe adicionados, como seja o envio de equipas de técnicos a um país membro ou parceiro que o solicite e que esteja sujeito a uma ameaça cibernética para a qual não tenha capacidade de resposta.

A NATO é ainda capaz de oferecer, mediante solicitação, assistência profissional e bem organizada, na edificação e melhoria das capacidades ciberdefesa dos seus membros e parceiros, especialmente aqueles que não têm recursos para configurar as suas. Esta oferta é constituída por peritos, que podem executar missões de suporte real, em coordenação com os peritos nacionais.

Na Cimeira de Lisboa, em Novembro de 2010, a NATO aprovou o atual Conceito Estratégico. No seu ponto 19 sobre a defesa e dissuasão, estabeleceu-se que a NATO garantiria os vetores necessários para desenvolver ainda mais a sua capacidade para prevenir, detetar, defender e recuperar de ataques pelo ciberespaço. Neste âmbito está prevista a utilização do processo de planeamento NATO, para reforçar e coordenar as capacidades nacionais de defesa do ciberespaço, colocando todos os organismos aliados sob "*cyber protection*" centralizada, e integrando melhor a visão do Ciberespaço, a "*NATO cyber awareness*", e o sistema de alerta e resposta com os países membros (NATO, 2010).

Propôs-se, ainda, apoiar esforços no sentido de desenvolver uma efetiva regulação internacional, no modo como os "*Internet Service Providers*" (ISP) tratam o código malicioso, e na adoção de um mínimo de protocolos de segurança para os computadores autorizados a utilizar os serviços dos ISP.

Em 2010, o *Allied Command Transformation (ACT)* definiu o *Framework for Collaborative Interaction (FFCI)*, que permite à NATO e às empresas privadas de cibersegurança trabalhar em conjunto, no desenvolvimento de produtos. Estas, tem sido convidadas para participar em eventos NATO relacionados com a cibersegurança, tal como o *Information Assurance Symposium*, onde os diferentes palestrantes compartilham os seus conhecimentos com os delegados de diferentes países da NATO. Sem a cooperação com a indústria privada, as redes da Aliança estariam, quase certamente, comprometidas.

Ainda no âmbito do treino e preparação dos seus aliados, a NATO realiza anualmente, diversos exercícios de ciberdefesa com os seus membros, nos quais Portugal tem participado, tais como o *Cyber Coalition* e o *Cyber Endeavor.*

Em síntese, a NATO desenvolve um conjunto de atividades de base doutrinária, operacional, técnica, jurídica e formativa em cooperação com os seus membros e parceiros, que lhes têm servido de catalisador no desenvolvimento das suas cibercapacidades.

e. Síntese conclusiva.

Constata-se, que em Portugal não existe ainda uma ENSI nem um CNC o que dificulta, por falta de enquadramento, as atividades de cooperação e partilha e a operacionalidade para enfrentar os ciberataques. A função de CERT nacional tem sido desenvolvida pelo CERT.pt e é com esta entidade que o CC-CRISI do EMGFA estabeleceu um protocolo, com o qual tem desenvolvido algumas ações de partilha e cooperação técnica.

As FFAA, têm também desenvolvido diversas atividades de cooperação no âmbito da cibersegurança e ciberdefesa, não só entre si, mas também com a NATO e a UE, nomeadamente com a realização de exercícios e a participação em seminários e *workgroups* internacionais.

Julgamos no entanto, que as áreas de cooperação são ainda bastante limitadas, tomando em consideração, o número de militares envolvidos e a quantidade de ações que atualmente se efetuam, face às que potencialmente poderão ser realizadas[32].

[32] Este aspeto tornar-se-á ainda mais evidente, ao longo deste trabalho, quando identificarmos as áreas potenciais de cooperação para as FFAA.

Assim, perante a formulação da QD2 – "Como é que a capacidade de ciberdefesa já desenvolvida pelas FFAA, contribui para a cooperação internacional?" Confirma-se que esta capacidade não estando ainda plenamente desenvolvida nas FFAA, implica consequentemente uma menor participação em diversas áreas da cooperação e a validação da H2 – "A cooperação entre as FFAA e outras organizações é reduzida".

3. Áreas em que a cooperação se poderá desenvolver.

Após o ciberataque efetuado à Estónia em Maio de 2007 e a tomada de consciência da dimensão real do problema que estava a decorrer, os responsáveis governamentais, reuniram um gabinete de crise, no qual tomou parte o então recém-criado CERT-EE[33]. Aplicaram-se inicialmente algumas medidas nacionais, que tiveram um efeito muito limitado. Rapidamente perceberam que só com uma ampla cooperação internacional seria possível dar uma resposta eficaz ao ataque a que estavam a ser sujeitos. Com o apoio das equipas eslovena (CERT.SI), alemã (DFN-CERT) e finlandesa (CERT.FI), conjugado e coordenado com os maiores ISP e alguns peritos da época, foi possível dar uma resposta eficaz ao ciberataque a que o país tinha sido sujeito.

Não foi a primeira vez em que a cooperação internacional contra os ciberataques na Europa mostrou a sua eficácia. A novidade foi constatar-se que só após uma elevada resposta cooperativa, foi possível repor a soberania de um país.

Os ciberataques não têm fronteiras e a mitigação dos seus efeitos está associada à coordenação e à cooperação nacional ou internacional. Esta, será concretizada envolvendo toda a comunidade à escala global, as equipas de segurança das TIC, os CERTs nacionais e de uma forma geral todas as entidades com responsabilidade na segurança dos sistemas de informação.

As iniciativas de cooperação internacional, pressupõem a existência de uma estratégia de cibersegurança nacional que sirva de suporte às áreas com interesse a desenvolver. A cooperação não é afinal um fim em sim mesmo, mas apenas a forma de abordar com mais eficiência e eficácia a problemática das ciberameaças e dos ciberataques.

Um dos aspetos analisados ao longo deste trabalho que se tomou em consideração, foi a forma como a cooperação é desenvolvida atualmente entre os CERT mundiais. Existe uma vasta gama de informações disponíveis na web acerca dos CERT dos países, sendo a mais comum, a partilha de informação técnica sobre as pragas cibernéticas, as técnicas para as eliminar e as respetivas informações estatísticas.

Em resultado da conjugação destes estudos, identificaram-se diversas áreas em que já são desenvolvidas ações de cooperação ou com potencial para o serem:

a. A partilha das características das ameaças.

De forma generalizada já se concretiza esta ação, que consiste na partilha das características técnicas das ameaças ao ciberespaço que decorrem num determinado

[33] CERT da Estónia.

momento. Porém, nem sempre as equipas conseguem compartilhar todos os dados dos incidentes da forma que seria necessário. Verifica-se que devido à diversa regulamentação dos países em relação à manipulação dos dados, existem diferentes tratamentos, que dificultam a sua partilha. A classificação de segurança dos dados, a criticidade da informação ou o grau de evasão de uma ameaça, são barreiras à partilha generalizada, mesmo entre CERTs, que as comunidades têm tentado ultrapassar.

Associados a esta problemática têm-se desenvolvido esforços no sentido de criar padrões e formatos de troca de informação sobre incidentes informáticos que permitam agilizar a sua resposta.

No caso particular das FFAA, este especto é ainda mais crítico já que, por natureza, grande parte da informação que é transferida nos SI das FFAA é classificada, exigindo uma definição clara das regras de partilha.

b. A troca de dados estatísticos.

Com o número de incidentes organizados por diferentes classes, permite-se observar padrões e tendências dos ciberataques, assim como prever ataques futuros em larga escala, informações estas bastante uteis aos analistas. Atualmente não existe uma normalização no tratamento dos dados estatísticos o que dificulta uma análise comum. Esta tarefa exige também, o desenvolvimento e implementação de uma norma de classificação comum, percetível e tratável pelas diferentes equipas nacionais e internacionais, constituindo-se como um objetivo a atingir.

c. *A situation awareness picture.*

Há a necessidade de ter em permanência aquilo que se designa por *"situation awareness picture",* com a capacidade de monitorizar os acontecimentos a cada instante no ciberespaço, de antecipar ataques e eventos, de reconhecer eventos não planeados na rede, de analisar e escolher respostas defensivas em função das ameaças. "*É necessário que alguém compreenda o que está a acontecer, o que está prestes a acontecer e o que já aconteceu. Uma tal perceção da situação, inclui a compreensão do campo de batalha, a identificação das possíveis ameaças, e os riscos que colocam. Inclui ainda uma priorização da ameaça, o conhecimento das capacidades amigas, as suas vulnerabilidades e o estado operacional atual*" (Melo, 2011).

"No Ciberespaço, não existe atualmente uma entidade que tenha a capacidade ou autoridade para manter o nível de detalhe necessário na perceção da situação, garantindo um acesso ininterrupto ao Ciberespaço. A perceção da situação, depende da troca de

informação entre um vasto leque de entidades, desde parceiros internacionais, agências governamentais, indústria, meios académicos, e mesmo utilizadores individuais". (Keys, 2009 cit. por Melo, 2011). Os CERT nacionais e internacionais terão também um papel relevante na maximização desta capacidade, quando efetuam troca de informação entre os mesmos. O estabelecimento da "*situation awareness picture*" deve ser um atributo para qualquer núcleo CERT.

O desafio a este nível passará por aplicar as melhores práticas no âmbito da cooperação, em envolver recursos humanos especializados, em escolher as plataformas tecnologicamente mais adequadas e interoperáveis internacionalmente, tendencialmente de forma automática, apoiadas em canais tão abertos quanto possível para troca de informação, que permitam obter em permanência uma *Common Operational Picture* (COP) do ciberespaço e dar uma resposta eficaz às ciberameaças.

"*É também esta perceção do estado da rede, dos computadores que formam a rede e dos programas que neles correm, que contribuirá para o aumento da confiança e segurança, na utilização do Ciberespaço no apoio às operações militares executadas pelos Ramos"* (Melo, 2011)

É também percetível, que, quanto maior for o número de entidades que possam dar informação através de uma plataforma comum em tempo real, melhor será necessariamente a "*situation awareness".*

d. A normalização e a certificação.

A normalização e certificação de produtos e serviços na área da cibersegurança trarão vantagens reconhecidas. *"A adoção de um conjunto de normas estabelece a utilização de uma taxonomia e cria um referencial de medida que permite a avaliação e a fiscalização do seu objeto. Desta forma, a normalização reduz ambiguidades, facilita a comunicação e a cooperação entre agentes, sejam eles entidades privadas ou de Estados, para além de promoverem o ambiente de confiança à interoperabilidade e à cooperação"*(Santos, 2011).

Existem várias organizações que produzem normas com maior ou menor aplicabilidade aos produtos e serviços no âmbito da cibersegurança. Ressaltam-se a família de normas da *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 27001 em que se definem modelos de gestão de segurança da informação com aplicabilidade em qualquer tipo de organismo. Muitas destas

normas estão orientadas para a certificação de produtos e serviços que são desenvolvidos posteriormente pela indústria.

Os desenvolvimentos destes normativos pressupõem a participação de toda a comunidade que está envolvida na problemática do ciberespaço, melhorando a interoperabilidade e a cooperação mundial.

e. As boas práticas internacionais.

Em contraponto às dificuldades em desenvolver, aprovar e implementar normas que se adequem às alterações muito rápidas das ciberameças, as comunidades optam também por difundir boas práticas. "*Sem o peso institucional de uma norma a elaboração de boas práticas é muitas vezes feita pela parte interessada no âmbito de grupos de trabalho mais ou menos formais, num ambiente colaborativo e de partilha*" (Santos, 2011, 53). Tem sido neste cenário de partilha de boas práticas que se tem estabelecido um ambiente de confiança, que tem permitido ultrapassar alguns dos problemas colocados pelas ciberameças e que interessa manter ou desenvolver.

f. A análise forense.

Apoiada em equipamentos e aplicações específicas, esta análise consiste num conjunto de técnicas para coligir e examinar dados e assinaturas digitais, reconstruir ciberataques e identificar e rastrear invasões aos sistemas de informação. As dificuldades nesta análise, estão ligadas à elevada diversidade de tecnologias utilizadas, à encriptação dos dados, a ficheiros apagados de difícil recuperação, à análise em tempo útil de dados admissíveis em sede de prova, aos aspetos de transnacionalidade do delito informático e ao enquadramento jurídico-legal aplicável para cada uma destas situações (Santos, 2011).

g. A simulação.

A simulação de cenários de ciberataques em sala, apoiada em ferramentas específicas, também é um ganho acrescido, na medida em que permite aumentar o conhecimento e a especialização, na resposta aos incidentes informáticos.

Esta capacidade exige meios dispendiosos e técnicos, que convenientemente partilhados, poderão racionalizar esta atividade.

Perspetiva-se a criação de um simulador que sirva as FFAA no seu conjunto, e que possa ser partilhado pelos Ramos e eventualmente com outros países, como forma de contrapartida a outras áreas da ciberdefesa.

h. O treino de novas equipas.

A assistência e o apoio às novas equipas, desenvolvida dentro e fora das organizações, muitas vezes internacionalmente, têm sido considerados cruciais para o sucesso da segurança das SI/TIC. Nesta linha de ação, as equipas mais experientes fornecem orientação e divulgam as melhores práticas para as equipas em formação, incluindo visitas aos locais de trabalho e às empresas, tutoriais e intercâmbio entre especialistas capazes de identificar e satisfazer as suas necessidades. Esta forma de partilha acelera o processo de aquisição, a capacidade de reação e o domínio de conhecimentos, dentro das organizações de segurança das SI/TIC.

i. O direito no ciberespaço.

O desenvolvimento do direito internacional aplicável a operações cibernéticas, tem preocupações e inclui questões como a possibilidade do uso da força, o direito de autodefesa, contramedidas, o "*jus ad bellum" (*O direito internacional que rege o recurso à força pelos Estados, como instrumento de sua política nacional) e o "*jus in bello" (O* direito internacional que regula a conduta dos conflitos armados, também rotulados de lei da guerra, a lei de conflito armado, ou do direito humanitário internacional), a lei de atribuição de neutralidade e de responsabilidade do Estado ou questões emergentes como as implicações legais da utilização automática em resposta a incidentes.

No âmbito desta problemática têm sido desenvolvidas diversas iniciativas. O Manual de Tallinn (Schmitt, 2013), sobre o Direito Internacional aplicável a *Cyberwarfare*, escrito a convite do Centro por um grupo de independentes, "Grupo Internacional de Peritos", é o resultado de um esforço de três anos para examinar as normas existentes de direito internacional aplicável a esta nova forma de guerra. O Manual de Tallinn presta especial atenção ao "*jus ad bellum"*, e ao "*jus in bello"* e a responsabilidade do Estado, são tratados no contexto desses temas. Paralelamente realizam-se seminários e conferencias sobre a mesma problemática sob a égide da NATO e outras entidades como a ENISA.

Prevê-se que o desenvolvimento e harmonização de leis aplicáveis no âmbito da ciberdefesa e cibersegurança e adequadas à sua complexidade e evolução, sejam um dos desafios futuros mais complexos à cooperação internacional.

j. A rede de alertas internacional.

O estabelecimento das informações dos sensores IDS, ligados a servidores centrais, permitem às equipas correlacionar alertas gerados nas suas redes com as de outras. Para facilitar a comunicação entre equipas, deverão existir canais seguros e confiáveis para a

distribuição de alertas. Este tipo de serviço exige protocolos e/ou formulários normalizados e de confiança, mas representa um ganho acrescido para as entidades que os conseguem estabelecer.

k. A investigação e desenvolvimento.

A investigação e desenvolvimento, fundamental na capacidade de reação a novas ameaças cibernéticas, têm de estar envolvidas numa parceria muito estreita, com os núcleos de reação aos ciberataques e à indústria. O desenvolvimento de novos produtos ou estratégias de cibersegurança, quer sejam equipamentos ou *software* aplicacional, só terá viabilidade económica e realmente eficaz, desde que a sua evolução acompanhe o combate às novas pragas cibernéticas, preferencialmente em tempo real. As empresas tradicionalmente dedicadas a produtos antivírus[34], *firewalls*, IDS, ou de equipamentos específicos para a ciberdefesa, têm demonstrado ser capazes de produzir software de proteção adequado às necessidades que até agora se têm manifestado.

"*A participação da indústria, dos privados, nesta matéria, deve neste domínio de tecnicidade, ser de caráter supletivo, e perante requisitos bem definidos pelo estado."* (Aires, 2012). Percebe-se que face à complexidade das novas gerações de vírus informáticos e às novas tipologias dos ciberataques, a indústria terá que estabelecer uma cooperação efetiva com todas as entidades que estão no terreno com capacidade de deteção e monitorização cibernética, com as universidades e os centros académicos que existem a nível mundial, de forma a proporcionar produtos cada vez mais eficazes e em tempo real.

l. A doutrina.

A difusão/elaboração de doutrina, regulamentações e a difusão de boas práticas nesta área será um dos vetores de desenvolvimento com maior relevância. Atualmente já existe doutrina ao nível da NATO e de normas regulamentadoras na operacionalização dos CERT, que conjugadas com boas práticas aceites nestas comunidades, têm permitido a operacionalização de forma cooperativa, à resposta aos incidentes informáticos. A UE, tem de igual forma difundido diretrizes e boas práticas de mitigação de riscos.

Nesta linha de raciocínio, todos os países membros, quer seja da NATO, da UE ou outra organização, poderão dar a sua contribuição, sendo possível no limite, desenvolver doutrina aceite internacionalmente.

[34] São exemplos destas empresas a *AVAST, AVG, Norton, Kaspersky, Sophos, PANDA, BitDefender*.

m. Os exercícios de ciberdefesa.

O treino é fundamental no desenvolvimento e manutenção do nível de capacidade de resposta aos incidentes informáticos, para todas as entidades envolvidas. A NATO divulgou em 4 de fevereiro de 2013 o documento, " *NATO Cyber Defence (CD) Education and Trainning Concept*", que dá um enquadramento conceptual ao treino de forças no âmbito da ciberdefesa e está em consonância com o *Training Requirements Analysis (TRA) and Training Needs Analysis (TNA).*

Como forma de melhorar o treino, os elementos das FFAA têm participado anualmente em diversos exercícios de cibersegurança e ciberdefesa, tais como o "*Cyber Coalition*" da NATO, o "*Cyber Europe 2012*" da ENISA ou o "*Ciber Perseu*" organizado pelo Exército. São criados cenários que incluem simultaneamente diversos tipos de ciberataques como, ataques de *e-mail*, *phishing*, infeção de sites *web* com *malware*[35], ataques DDoS[36] e ciberespionagem entre outros. A maioria dos incidentes exige ações, coordenação e cooperação entre os participantes. São dirigidos a especialistas de segurança em SI, operadores de telecomunicações, ISP, instituições financeiras, organismos públicos e decisores com responsabilidades nas SI/TIC, sejam militares ou civis.

Estes exercícios visam desenvolver o conhecimento para aumentar o nível de resiliência das infraestruturas críticas de informação, testar a capacidade de resposta a incidentes, desenvolver a capacidade de cooperação e aplicar estratégias e boas práticas nestas áreas.

n. A formação.

As sociedades da informação e do conhecimento estão intrinsecamente ligados a uma cultura de segurança em que todos, desde os cidadãos, passando pelas organizações, até aos estados, terão que estar não só consciencializados, mas também formados e preparados para estarem à altura de responderem aos perigos do ciberespaço. A formação em segurança dos sistemas de informação e particularmente na cibersegurança, é assim um pilar básico na estruturação da cultura de segurança, em qualquer sociedade ou organização. A nível nacional, a oferta de formação na área da cibersegurança tem aumentado nos meios académicos, em escolas técnicas de formação, mas também pelas empresas que vendem equipamentos e soluções contra as ciberameaças e que associam estrategicamente pacotes de formação a essas mesmas soluções.

[35] *Malicious software.*
[36] *Distributed Denial of Service*.

Os membros da NATO têm a possibilidade de frequentar os cursos do CCDOE, onde são exigidos perfis de conhecimentos iniciais bastante elevados em TIC aos seus alunos e os cursos são reconhecidos pela qualidade dos conhecimentos adquiridos. Mas é sobretudo a oportunidade e a possibilidade de adquirir conhecimentos e competências, em concordância com um padrão institucional de grande excelência, que deve ser aproveitado por todos os membros da NATO.

o. A governação da cibersegurança.

A nível nacional ainda não foi aprovada a ENSI nem a consequente ENC e o CNC apenas se prevê que entre em funcionamento durante este ano. Paralelamente, existem a nível nacional entidades, cujas capacidades e valências, conferem globalmente a base para uma resposta aos ataques informáticos[37]. Tomando isto em consideração, percebe-se a necessidade da existência de uma governação da cibersegurança, que consiga coordenar e congregar todas as capacidades e competências, para que não existam áreas de sobreposição nem desperdício ou ineficiência na utilização dos recursos e que se consiga orientar o esforço a nível nacional, em concordância com as linhas de orientação internacionais nesta área.

As FFAA terão que desenvolver o seu papel a nível nacional, tomando sempre em consideração a sua especificidade, não esquecendo que fazem também parte de organizações internacionais, com quem têm compromissos assumidos.

p. Apoio no desenvolvimento da capacidade de cibersegurança/ciberdefesa.

A comunidade internacional, através das suas organizações como a NATO, a ENISA e até os CERT internacionais, têm oferecido equipas, que com os seus conhecimentos e com as suas experiências, apoiam a construção das capacidade de cibersegurança e ciberdefesa nacionais, aos países membros, evidenciando assim mais um modo de partilha e cooperação.

q. Síntese conclusiva

Analisaram-se alguns aspetos de cooperação que já se concretizam presentemente e desenvolveu-se uma pesquisa no sentido de se determinar novas áreas em que esta cooperação será desejável. É percetível que perante as ameaças no ciberespaço cada vez mais diversificadas e com maior impacto nas sociedades, também as áreas de cooperação terão que ser cada vez mais elevadas, como estratégia mais eficaz no combate aos ciberataques

[37] Em Anexo C: Entidades relevantes na cibersegurança em Portugal.

Ainda não existe uma estratégia de cibersegurança nacional, o que dificulta a definição de áreas e linhas de ação no desenvolvimento da ciberdefesa cooperativa.

Das áreas de cooperação identificadas, confirma-se que as FFAA já efetuam partilha de dados técnicos sobre os ataques cibernéticos, participam em exercícios nacionais e no âmbito da NATO e que têm desenvolvido esforços na formação dos seus militares.

A NATO, a ENISA e os CERT internacionais, entre outras entidades, têm uma oferta bastante larga em áreas de cooperação, nas quais as FFAA poderão participar. Consideramos que a formação, a partilha de informação técnica sobre ciberameças e de dados estatísticos e a contribuição para o estabelecimento da *situation awareness picture*, poderão ser as áreas prioritárias, que desenvolveriam competências técnicas, conhecimento e confiança aos elementos das FFAA.

Consideramos que em resposta à QD3 – "Quais as áreas de cooperação internacional de ciberdefesa que são desejáveis pelas FFAA?" foi possível identificar um elevado numero de áreas, em que potencialmente as FFAA poderão participar cooperativamente, além daquelas em que já participam atualmente. Neste contexto e tendo sido identificadas novas áreas de cooperação internacional para as FFAA, que contribuirão para a eliminação das ameaças cibernéticas transnacionais, consideramos validada a H3 – "Os ciberataques, não tendo fronteiras, exigem a definição de áreas comuns de cooperação internacional".

4. Desenvolvimento da ciberdefesa cooperativa nas FFAA

A cooperação não sendo um fim em si mesmo, é certamente a forma como a comunidade internacional se tem organizado para combater as pragas cibernéticas.

Coloca-se a questão de saber quais as componentes, que deverão as FFAA desenvolver para que a cooperação seja aumentada e mais efetiva.

No desenvolvimento de capacidades nas FFAA tem sido utilizado o acrónimo composto pelos termos Doutrina, Organização, Treino, Material, Interoperabilidade, Liderança, Pessoal e Infraestruturas (DOTMILPI)[38], pelo que iremos desenvolver os aspetos com maior aplicabilidade neste contexto.

a. Doutrina

Relativamente à doutrina de ciberdefesa, o conhecimento conceptual e organizacional está difundido através das publicações emanadas pelo EMGFA, Marinha e Força Aérea. O Exército apoia-se no seu documento "Elemento da guerra da informação, estudo e implicações" (EME, 2008).

Existe a nível nacional documentação na área do Infosec[39] que serve de referência, na construção de conhecimento doutrinário

O Exército está a preparar documentação que definirá procedimentos, técnicas e táticas aplicáveis às CNO.

A nível NATO, é aplicável a doutrina de referência definida no AJP 3.10 *Informations Operations*, em que estão previstas as CNO no âmbito operacional. Na ausência de doutrina nacional também poderão ser aplicadas.

b. Organização

Atualmente as FFAA apresentam uma estrutura organizacional, que está implementada em três níveis: doutrinário, operacional e de utilizador, orientados para a cibersegurança. Nesta data só o Exército possui um módulo tático, que consolida a implementação de uma capacidade de ciberdefesa. A Marinha pretende melhorar e consolidar a sua capacidade de cibersegurança, através da implementação de um sistema de correlação e gestão de incidentes e um laboratório forense.

O desenvolvimento organizacional das estruturas dedicadas à cibersegurança e ciberdefesa, deverão tomar em consideração os meios e as estruturas existentes e os

[38] Tem-se utilizado regularmente, este acrónimo, na abordagem ao desenvolvimento de capacidades na NATO.
[39] Documento da segurança da informação (INFOSEC) RAD 280-1 e compreende a segurança dos computadores, comunicações e redes.

conceitos de capacidade de resposta a incidentes informáticos já emanados pelos Ramos através das suas publicações.

A montante, deverá ser considerado um conceito mais vasto de desenvolvimento de uma capacidade de superioridade da informação, dentro da qual a estrutura de ciberdefesa será um dos pilares de sustentação a ser construído.

Também desejavelmente a capacidade de ciberdefesa poderá ser desenvolvida numa perspetiva conjunta, de forma a catalisar sinergias entre os Ramos e melhorar a eficiência na resposta a incidentes. ”*Não temos dimensão para termos esta capacidade espartilhada por vários Ramos”* (Aires, 2012). Nesta perspetiva poderá ser colocada a hipótese de existir um único CERT, caso as FFAA efetuem a administração dos seus sistemas de informação de forma centralizada a partir de um dos Ramos ou no EMGFA.

Por exemplo as CNO, já desenvolvidas no Exército, poderão ser lideradas por este ramo evitando duplicação de meios.

c. Treino

O EMGFA, através do PEMGFA CSI 301, define os requisitos de formação e treino, relativamente ao pessoal envolvido na estrutura e organização da CRISI e nas atividades relacionadas com o tratamento e resposta a incidentes, uso de ferramentas e análise de vulnerabilidades, os níveis de credenciação nacional e NATO, necessários para o desempenho de funções neste domínio, bem como, o estabelecimento de relações de cooperação com entidades nacionais e internacionais, e em particular com a NATO (EMGFA, 2008).

No que diz respeito ao treino conjunto no domínio do ciberespaço, de destacar o exercício de ciberdefesa denominado “*Cyber Coalition”*, da NATO, no qual Portugal tem participado, envolvendo várias nações pertencentes a esta organização, com o objetivo de testar as capacidade técnicas e operacionais da Aliança, face a um ataque em larga escala. Neste tipo de exercícios, todas as nações participantes têm de lidar com ciberataques simulados. Os cenários deste género de exercícios requerem ação, coordenação e colaboração de especialistas de ciberdefesa e órgãos de gestão. Uma das mais-valias destes exercícios é a oportunidade de participarem todos os Ramos do país e de vários países, com militares e civis, o que dá uma perspetiva conjunta e combinada, extremamente enriquecedora em termos de troca de conhecimentos e experiências nesta área.

Durante o ano de 2012, o Exército organizou pela primeira vez o exercício nacional “*Cyber Perseu*”, no qual foi testado o módulo tático CIRC do Exército e em que os

restantes Ramos participaram como observadores. Exercícios deste género irão certamente realizar-se novamente, podendo ser associados a planos de contingência previamente aprovados, ou inseridos no âmbito do planeamento dos exercícios nacionais, constituindo uma excelente forma de desenvolver as capacidades e competências dos militares do Exército e dos restantes Ramos e sempre que possível de forma conjunta.

Também não poderá ser esquecida a necessidade de participar em exercícios[40] ou efetuar treino em conjugação com entidades civis nacionais e internacionais, de forma a desenvolver princípios de cooperação e competências na resolução de incidentes informáticos.

d. Material

A aquisição de equipamentos e *software* aplicacional especifico para a cibersegurança e ciberdefesa, deverá obedecer a requisitos técnicos normalizados internacionalmente e ser certificado, de forma a permitir a monitorização e a partilha de dados de forma interoperável entre Ramos e o EMGFA.

A partilha de dados com entidades exteriores às FFAA, terá que obedecer a requisitos previamente definidos que prevejam a especificidade das informações técnicas, seguramente classificados.

A capacidade de monitorização dos sistemas a implementar deve ser tal que permita obter permanentemente uma "*situation awareness*", com uma arquitetura que aceite indicações e forneça avisos ou alertas. Para tal, deve ter a possibilidade de monitorizar os acontecimentos correntes no ciberespaço e a compatibilidade na rede, antecipar ataques e eventos, reconhecer eventos não planeados na rede, iniciar precocemente a análise de ações alternativas, em resposta a ameaças detetadas e escolher respostas defensivas efetivas.

e. Interoperabilidade

A interoperabilidade será alcançada considerando dois aspetos fundamentais: tecnicamente, permitir a troca automática de dados entre sistemas de monitorização e controlo, com sistemas normalizados, certificados, filtrados e de acordo com regras previamente determinadas. Operacionalmente, desde que o seu uso seja baseado em doutrina, *standards*, regulamentos ou, no mínimo, procedimentos fundamentados em boas práticas, que permitam a fluidez de informação interna e externa. Neste âmbito, os

[40] O exercício *Cyber Europe* 2012 promovido pela ENISA é um exemplo em que participaram cerca de 25 países e várias centenas de organizações, como forma de desenvolver a capacidade de resiliência aos ciberataques e melhorar as competências dos participantes na resolução de incidentes informáticos.

protocolos de partilha de conhecimentos sobre incidentes informáticos entre o EMGFA e o CERT.pt, e a NATO, têm materializado este princípio.

f. Liderança

A liderança de cada um dos Ramos tem permitido o desenvolvimento das capacidades de ciberdefesa, de forma diferenciada em cada um deles.

Esta é uma área em que a partilha de recursos humanos e materiais, conjugados com uma política comum, poderia trazer racionalidade, coerência no modelo a desenvolver e uma adequação ao mundo real desta capacidade.

Consideramos assim que para haver um desenvolvimento partilhado, coordenado e coerente a liderança no desenvolvimento desta capacidade deveria ser concretizada por um dos Ramos ou pelo EMGFA.

g. Pessoal

Terá que existir pessoal em quantidade tal que permita o funcionamento das estruturas a 24/7, com a formação técnica adequada. O aspeto mais complexo que se prevê não serão tanto os quantitativos mas antes a sua especialização, exigente em termos de conhecimentos técnicos e operacionais, objetivo sempre difícil de alcançar atendendo a que os militares das FFAA tipicamente são obrigados a grandes rotações nas funções que ocupam, em curtos espaços de tempo.

Considera-se com potencial de partilha e cooperação, a formação técnica em segurança que é ministrado pelos Ramos, nas suas escolas técnicas de comunicações. No Exército é possível ministrar formações em cooperação com *partners*, como os cursos da CISCO na EPT. O Exército ministra ainda na Academia Militar um mestrado em Guerra da Informação, que pode ser frequentado por militares de todos os Ramos.

Internacionalmente, a NATO CIS School em Latina, Itália, ministra cursos na área da segurança dos sistemas de informações e comunicações a todos os países da aliança. Está prevista a vinda desta escola para Oeiras, onde se encontra atualmente o JHQ Lisbon, possibilitando eventualmente, a formação dos militares portugueses com custos mais reduzidos.

O NATO CCDCOE[41] em Tallin, ministra um conjunto de especializações avançadas em cibersegurança e ciberdefesa também a todos os países da NATO, pelo que

[41]O NATO CCDCOE além da formação, planeia exercícios, realiza seminários e desenvolve publicações em cibersegurança e ciberdefesa, aos seus aliados na NATO.

deve ser considerado o envio no curto prazo de militares para frequentar estes cursos em Tallin.

Desejavelmente, deve ser considerada a formação em segurança de SI, em escolas civis, pelos militares. Em alternativa, poderão ser estabelecidos protocolos que possam rentabilizar estas formações, já que previsivelmente são caras e têm que se realizar de forma contínua.

h. Infraestrutura

Neste subcapítulo devemos considerar a criação de instalações que permitam o desenvolvimento das atividades de administração e controle da RCFM e a segurança do SIC prioritariamente. Considerar ainda a criação de condições para o aumento do conhecimento sobre ciberataques e resposta aos mesmos, em ambiente de sala de aula, com a possibilidade de troca de experiencias e conhecimentos. Prever ainda a implementação de salas de simulação e laboratórios, que permitirão desenvolver os estudos e a investigação acerca de incidentes informáticos.

Por último, considerar que a RCFM é gerida e administrada pelo EMGFA e pelos Ramos, garantindo a disponibilização dos serviços de voz, mensagens e dados através de uma infraestrutura de comunicações baseada em diversas tecnologia (Fibra, cobre, micro-ondas). Em termos de arquitetura, deve permitir a gestão das redes e ferramentas básicas de proteção da informação, incluindo *firewalls*, antivírus e deteção de intrusão e sobretudo possibilitar uma gestão hierarquizada da rede, de forma a permitir a sua reconfiguração quando necessário, com reencaminhamentos varáveis, aumentando assim a resiliência aos ataques informáticos.

i. Síntese conclusiva

Como ideia base para a estruturação do desenvolvimento da capacidade de ciberdefesa nas FFAA servimo-nos do acrónimo DOTMILPI. Analisámos, assim, os aspetos e as características das componentes a desenvolver para uma capacidade efetiva de ciberdefesa nas FFAA.

Considera-se que só com aumento das competências e das capacidades dos meios humanos e materiais alocados à ciberdefesa, será possível desenvolver uma cooperação internacional mais efetiva, num maior número de áreas e de forma credível para as FFAA portuguesas, com retorno e uma melhoria real na eliminação das ameaças cibernéticas.

Assim perante a QD4 – "Quais as componentes a desenvolver pelas FFAA para que se atinja a ciberdefesa cooperativa de forma desejável?" confirma-se a H4-"As

componentes a desenvolver no estabelecimento de uma ciberdefesa cooperativa internacional deverão permitir a partilha de informações técnicas, a normalização de procedimentos e a formação e treino", mas relevamos também a importância e o impacto das componentes elencadas, nas restantes áreas de cooperação, vitais para o desenvolvimento da capacidade de ciberdefesa.

Conclusões.

O ciberespaço é hoje uma fonte de crescimento e oportunidades para as sociedades de uma forma geral e para as FFAA de uma forma particular. No entanto, a utilização do mesmo espaço de forma ilícita, as designadas ameaças ao ciberespaço, têm trazido à ordem do dia um conjunto de preocupações para as organizações, os estados.

É neste contexto, num mundo sem fronteiras como o ciberespaço, em que as FFAA cooperando internacionalmente com as suas capacidades, poderão ter um papel relevante na eliminação das ciberameaças, contribuindo para a manutenção da soberania nacional.

Como metodologia de investigação a esta problemática, recorreu-se à pesquisa documental e bibliográfica, através de consultas em biblioteca e na internet, complementada por entrevistas exploratórias, a partir das quais conseguiu-se determinar a QC-"De que forma as FFAA poderão desenvolver e aumentar a cooperação internacional na ciberdefesa" e as principais linhas de investigação:

— Avaliar as capacidades atuais de ciberdefesa das FFAA;
— Determinar como é que a ciberdefesa cooperativa é efetuada pelas FFAA;
— Determinar a nível internacional, quais as áreas da cooperação na ciberdefesa;
— Estimar quais as componentes a desenvolver, para que a cooperação na ciberdefesa aumente.

A investigação subsequente desenvolveu-se recorrendo à consulta de documentação nacional e internacional, difundida em livros, manuais, revistas especializadas ou através da internet e complementada por entrevistas a especialistas ou responsáveis pelos SIC das FFAA.

A comparação entre os resultados teóricos esperados, nas hipóteses, e os que efetivamente resultaram da análise dos dados obtidos, foram os seguintes:

Relativamente à HIP1:

Os resultados validaram esta hipótese pois concluiu-se que os Ramos encontram-se em diferentes estádios de consolidação e maturação da sua capacidade de proteção contra as ameaças no ciberespaço. Considerou-se que todos estão dotados uma capacidade de cibersegurança com um nível de desenvolvimento semelhantes e, só o Exército possui uma capacidade de ciberdefesa atualmente.

Relativamente à HIP2:

Confirmou-se que as FFAA desenvolvem em alguma áreas, atividades de cooperação de cibersegurança, a nível nacional e internacional. Constatou-se que partilham

informação sobre ciberameças e conhecimentos técnicos nesta área, entre si e com os CERT nacionais; participam em exercícios de ciberdefesa na NATO, EU e, frequentam fóruns e seminários internacionais relacionados com a problemática do ciberespaço.

A cooperação já realizada pelas FFAA reflete o esforço em desenvolver esta capacidade, mas potencialmente existem outras áreas com igual interesse, pelo que a HIP2 foi validada.

Relativamente à HIP3:

Esta hipótese, foi validada pelo facto de terem sido identificadas ao longo do trabalho, uma série de áreas em que a cooperação já se realiza internacionalmente, com maior ou menor desenvolvimento e participação das entidades responsáveis pelos SIC. Face à importância que têm, são de vital importância na construção e dinamização das capacidades de ciberdefesa.

Relativamente à HIP4:

Tomamos como base da análise o desenvolvimento das componentes de ciberdefesa, em torno do acrónimo DOTMILPI, a partir das quais consideramos que corresponderão um aumento efetivo das áreas de cooperação internacional, melhorando de forma efetiva a eliminação das ciberameaças, validando desta forma a HIP4.

A investigação realizada permitiu confirmar que a ameaça no ciberespaço é real, aumenta diariamente e torna-se cada vez mais complexa. O grau de sofisticação das ciberameças entrou num patamar, que as torna equivalentes às ameaças assimétricas, colocando em causa o funcionamento dos estados e da sua soberania.

As FFAA, têm um papel fundamental no contributo que poderão dar para eliminar as ameaças às infraestruturas críticas e aos organismos governamentais. Para tal, a capacidade de ciberdefesa das FFAA, que verificamos ser ainda insuficiente, terá que ser ainda mais desenvolvida, aumentando as competências e capacidades dos seus meios humanos e materiais.

A cooperação internacional é a forma unanimemente aceite e o desafio para um aumento efetivo da capacidade de exclusão das ameaças no ciberespaço. Nesta vertente, confirmamos que as FFAA são ainda limitadas na cooperação internacional que realizam, sendo um dos aspetos que terão que dinamizar necessariamente, para aumentar a sua credibilidade, na eliminação das ciberameaças.

Ao longo da investigação elencamos um conjunto de áreas possíveis para a cooperação, com níveis de desenvolvimento diferentes da comunidade internacional,

cabendo às FFAA determinar quais as mais importantes, para que nos contextos nacional e internacional, possam ser reconhecidos como parceiros efetivos na luta contra as ciberameaças.

No final deste trabalho, descriminamos um conjunto de vetores essenciais, que levarão necessariamente ao aumento das competências no domínio da ciberdefesa cooperativa internacional das FFAA dando resposta à QC enunciada no início deste trabalho.

-Contributos para o conhecimento. Considerações de ordem prática

A realização deste trabalho apoiado numa metodologia, desenvolvida em torno de um modelo previamente aceite, permitiu analisar e elencar de forma objetiva e sistemática, os aspetos que o caraterizam e as variáveis externas com impacto nas vertentes do tema deste estudo.

Desenvolveu-se uma avaliação sistemática e orientada sobre a problemática das capacidades de ciberdefesa cooperativa das FFAA e conseguiu-se elencar e sistematizar um conjunto de áreas possíveis de ser objeto de cooperação internacional, assim como os vetores de ação, para que essa cooperação seja aumentada.

O mundo cinético está a dar lugar ao cibernético. As ameaças ao ciberespaço são cada vez mais elevadas e com um impacto cada vez maior nas sociedades e nos estados. As FFAA são institucional e tecnicamente a entidade que, no limite, pode combinar de forma mais eficaz os meios cinéticos e de ciberdefesa, de forma a eliminar as pragas cibernéticas, também elas, tendencialmente conjugadas com ameaças assimétricas.

O tema deste trabalho, a cooperação internacional na ciberdefesa, não é um fim em si mesmo, mas um meio para se conseguir eficiência e eficácia na eliminação das ciberameças. Mas, o resultado positivo dessa cooperação só será efetivamente real, credível e percecionada pela sociedade, se as FFAA mostrarem competências e capacidades nesta área, que têm de ser desenvolvidas. Necessariamente hoje.

Bibliografia

Aires, MGen MJMC, 2012. *A ciberdefesa e a cooperação no EMGFA e nas FFAA*. Entrevistado por Cor Rui Pinto. Lisboa, 25 de Out. de 2012.

AJP 3_10 *Allied Joint Doutrine for Informations Operations* [Em linha]. Washington: Allied Joint Publication, 23 Novembro 2009. Disponível em: http://info.publicintelligence.net/NATO-IO.pdf, [Consult. 16 Nov. 2012].

Andress, J et al, 2011. *Cyber Warfare, techniques, tactics and tools for security practioners*. USA: Elsevier.

Amaral, P ,2008. *Top Secret*. *Como Proteger os Segredos da sua Empresa e Vigiar os Seus Concorrentes*. Alfragide: Academia do Livro.

Alexander, K, 2010. *Statement of General Keith Alexander, Commander United States Cyber Command before The House Committee on Armed Services* [Em linha]. Washington, 23 de Setembro de 2010. Disponível em: http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf, [Consult. 16 Set. 2012].

AR, 2005. Constituição da República Portuguesa (Lei Constitucional N.º 1/2005, de 12 de agosto). Sétima Revisão Constitucional. Lisboa: Diário da República.

CANALTECH, 2013. *Day-0: falha do Java deixa qualquer PC vulnerável e ainda não tem correção* [Em linha]. Brasil. Disponivel em: http://canaltech.com.br/noticia/seguranca/Day-0-Falha-do-Java-deixa-qualquer-PC-vulneravel-e-ainda-nao-tem-correcao/, [Consul. 14 Fev.2013].

CCDCOE, 2013. *Cooperative Cyber Defence Centre o Excellence Tallinn, Estonia* [Em linha]. Disponível em: http://ccdcoe.org/, [Consult.12 Fev 2013].

Coimbra, MGen D, 2012. *A ciberfesa e a cooperação nas FFAA*. Entrevistado por Cor Rui Pinto. Lisboa, 29 de Out. de 2012.

Damasio, CorTir L, 2012. A ciberdefesa e a cooperação internacional na Força Aérea. Entrevistado pelo Cor Rui Pinto. Lisboa, 10 de Dez. de 2012.

Dinis, J, 2009, *A guerra da Informação: Perspectivas de Segurança e Competitividade*. Lisboa: Revista Militar, artigo publicado em 18 de Junho de 2009.

EMA, 2012. PCA-16 Conceito de implementação da capacidade de resposta a incidentes de segurança da informação na Marinha. Lisboa, publicação do EMA de 16 Maio 2012.

EME, 2008. *Elemento da Guerra da Informação, Estruturas e Implicações*. Lisboa: Directiva do EME publicada em 21 Janeiro 2008.

EMGFA, 2008. *Organização e normas para a resposta a incidentes de segurança informática nas comunicações e sistemas de segurança das Forças Armadas.* Lisboa, publicação de 23 Setembro 2008.

ENISA, 2012a. *Inventory of CERT activities in Europe* [Em linha].. Disponivel em: http://www.enisa.europa.eu/, [Consult em 15 Jan. 2013].

ENISA, 2012b. ENISA Threat Landscape. [Em linha]. Disponível em: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape,[Consult. 18 Mar. 2013].

EXPRESSO, 2011. *Sistema Vigilis detecta 75 mil vulnerabilidades em Portugal.* [Em linha]. Lisboa, 4 de Janeiro de 2011. Disponível em: http://aeiou.expresso.pt/ataques-informaticos-sistema-vigilis-deteta-75-mil-vulnerabilidades-em-portugal=f624021, [Consult. 14 Nov. 2012].

Geers, K, 2012. *Strategic cyber security: evaluation nation-state cyber attack mitigation strategies with DEMATEL*. Dissertação em doutoramento. TUT.

GNS, 2012. Proposta de Estratégia Nacional de Cibersegurança, [Em linha]. Lisboa. Disponível em: http://www.gns.gov.pt/NR/rdonlyres/ED57762F-3556-4C05-9644-888E35C790BB/0/PropostaEstrat%C3%A9giaNacionaldeCiberseguran%C3%A7aPortuguesa.pdf, [Consult. 12 Nov. 2012].

Connolly, Cmdt C, 2013. *Cyber Security in the UK.* IDN, 28 de Fevereiro de 2013. Lisboa: IDN.

Governo, 2012a. *Resolução do Conselho de Ministros nº 12/2012 de 7 de fevereiro. Aprova o plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública*. [Em linha]. Disponível em: http://dre.pt/pdf1sdip/2012/02/02700/0059600605.pdf,[Consult. 28 Set. 2012].

Governo, 2012b. Resolução do Conselho de Ministros nº 112/2012 de 31 de dezembro. Aprova a Agenda Portugal Digital. [Em linha]. Disponível em: http://dre.pt/pdf1sdip/2012/12/25200/0730707319.pdf, [Consult. 20 Fev. de 2013].

Gzosseck, CG, 2012. *An evaluation of state-level strategies against bootnets in the context of ciberconflits*. Tese de doutoramento.EBS.

Hackmageddon, 2013: *Motivations behind attacks* [Em linha]. Disponivel em:http://hackmageddon.com/, [Consult. em 21 Abr. de 2013].

ITU, 2010. *Press release: 4.6 billion mobile subscriptions by the end of 2009* [Em linha]. .Genève: International Telecomunication Union, 6 de Outubro de 2009. Disponível em: http://www.itu.int/newsroom/press_releases/2009/39.html, [Consult. 12 Nov. 2012].

JP 1_02 , 2010. *Dictionary of Military and Associated Terms* [Em linha]. Washington: Joint Publication 1-02, 31 de Julho de 2010. Disponível em: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf , [Consult. 12 Nov. 2012].

JP 3_13, 2012. *Information Operations* [Em linha].Washington: Joint Publication 3_13, 27 de Novembro de 2012. Disponível em: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, [Consult. 12 Mar. 2013].

Keys, RonGen ML, 2009. *Concept for Possible Cyberspace Shared situational Awareness*. Washington: *Joint Concept Technology Demonstration*, 22 de Setembro de 2009.

Lynn, W, 2010. US deputy Defense Secretary, *Cyberwarfare Extends Scope of Conflit* [Em linha]. Washington: *American Forces Press Service*. Disponível em: http://www.defense.gov/news/newsarticle.aspx?id=61107 , [Consult. 12 Nov. 2012].

Mamede, H S, 2006. *Segurança informática nas organizações*. Lisboa: FCA.

Marques, Alm G, 2013. *A ciberdefesa e a cooperação internacional na Marinha*. Entrevistado por Cor Rui Pinto. Lisboa, 27 de Fev. de 2013.

Matias, MGen RMX, 2012. *A ciberdefesa e a cooperação internacional no Exército*. Entrevistado por Cor Rui Pinto. Lisboa, 24 de Out. de 2012.

Melo, Cor PJP, 2011. *A ciberguerra. Estrutura nacional para enfrentar as vulnerabilidades-uma capacidade militar autónoma ou partilhada*. Trabalho de investigação individual realizado no âmbito do Curso de Promoção a Oficial General 2010/11. IESM.

Melo, MGen PJP, 2012. *A ciberdefesa e a cooperação internacional nas FFAA*. Entrevistado pelo Cor Rui Pinto. Lisboa, 26 de Out. de 2012

MDN, 2012. *O desafio do ciberespaço: Grandes temas do Conceito Estratégico de defesa Nacional*. Universidade do Minho. 24 de Setembro de 2012. Braga: MDN

NATO,1949. *The North Atlantic Treaty* [Em linha]. Washington D.C. 4 de Abril de 1949. Disponível em: http://www.nato.int/cps/en/natolive/official_texts_17120.htm , [Consult. 12 Nov. 2012].

NATO, 2009. *Nato and Cyber Defence*, 173 DSFC 09 E bis . p 67[Em linha]. Bruxelas, 2011. Disponível em: http://www.nato-a.int/default.asp?SHORTCUT=1782, [Consult. 12 Nov. 2012].

NATO , 2010a. *NATO 2020 – Analysis and Recommendations of the Group of Experts on a new strategic Concept for NATO* [Em linha]. Bruxelas, 2010. Disponível em: http://www.nato.int/strategic-concept/expertsreport.pdf. , [Consult. 12 Nov. 2012].

NATO, 2010b. Strategic Concept For the Defense and Security of the Members of *the North Atlantic Treaty Organization.* [Em Linha]. Lisboa, 2010. Disponível em: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf , [Consult. 12 Nov. 2012].

NATO, 2011. *Defending the networks. The NATO Policy on Cyber Defence.*[Em linha]. Bruxelas, 2011. Disponível em: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf, [Consult. 12 Mar. 2013].

Nunes, PFV, 2009. *Ciberterrorismo: Aspectos de Segurança.* Lisboa: Revista Militar, 25 de Junho de 2009.

Nunes, PFV, 2012a. *A definição de uma Estratégia Nacional de Cibersegurança*. In Carriço, coord., 2012. Nação e Defesa. Cibersegurança. Lisboa: IDN. Nº 133, 5ª Serie, 133-127.

Nunes, PFV, 2012b. *O desafio do ciberespaço: Grandes temas do Conceito Estratégico de defesa Nacional*. Universidade do Minho. 24 de Setembro de 2012. Braga: MDN

Nunes, PFV, 2013. *A ciberdefesa e a cooperação internacional nas FFAA*. Entrevistado pelo Cor Rui Pinto. Lisboa, 8 de Abr. de 2013.

ONU , 1955. *Carta das Nações Unidas* [Em linha]. Nova Iorque: ONU,14 de Dezembro de 1955. Disponível em: http://www.fd.uc.pt/CI/CEE/pm/Tratados/carta-onu.htm, [Consult. 12 Nov. 2012].

Ottis, R, 2011. *A systematic approach to offensive volunteer cyber militia*. Dissertação no âmbito da obtenção do grau de doutor em Philosophy of Engineering. TUT.

Owens, WA et al, 2009. *Tecnology, Policy,Law, and Ethics Regarding U.S. Acquisition and Use of cyberattack capabilities*. Washington: The National Academies Press, 2009.

Quéméner, M, et al, 2009. *La Guerre du cyberspace aura bien lieu.* Paris: Defense nationale et sécurité collective. Março de 2009.

Ramos, João, 2011. *Primeiro Vírus Informático Criado há 40 Anos.* [Em linha]. Artigo na revista Expresso de 19 de Março de 2011. Disponível em : http://aeiou.expresso.pt/primeiro-virus-informatico-criado-ha-40-anos=f638343, [Consult. 12 Nov. 2012].

Santo, Gen E (2010). *Novo Ano,Novos Desafios: Ciberataques e Ciberdefesa*.[Em linha]. Lisboa: Revista Militar, editorial de Julho de 2010. Disponível em: http://www.revistamilitar.pt/modules/articles/article.php?id=533 ,[Consult. 12 Nov. 2012].

Santos, Gen JAL, 2009. *As Guerras Que Já Aí Estão e as Que Nos Esperam Se os Políticos não Mudarem.* Lisboa: Publicações Europa-América, Dezembro de 2009.

Santos, JLA, 2011. *Contributos para uma melhor governação da cibersegurança em Portugal.* Dissertação de Mestrado em Direito e Segurança. Universidade Nova de Lisboa.

Santos, P et al., 2008.*CYBERWAR o fenónemo, as tecnologias e os actores.* Lisboa: FCA

Schmitt, MN, ed. lit., 2013, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Nova Iorque, *Cambridge University Press.*

SIGNAL, 2012. *Cybersecurity, The threat goes viral* [Em linha]*:*AFCEA INTERNATIONAL JOURNAL, Agosto de 2012.

Silva, Cap NABM, 2012. *Segurança e defesa nacional: o desenvolvimento de capacidades de ciberdefesa*. Trabalho de investigação realizado no âmbito do Curso de Estado maior conjunto. IESM.

Sousa, CTen B, 2011. *Integração de fatores legais e estratégicos em ciber prontidão*. Trabalho de Investigação individual realizado no âmbito do Curso de Promoção a Oficial Superior -Marinha. IESM.

STRATCOM , 2010. *US Cyber Command* [Em linha]. United States Strategic Command, 2010. Disponível em: http://www.stratcom.mil/factsheets/cc/ ,[Consult. 12 Nov. 2012].

SYMANTEC, 2012. *Stux net 0.5: The Missing Link* [Em linha]. Symantec 2012. Disponivel em:http://www.symantec.com/connect/blogs/stuxnet-05-missing-link, [Consult. 26 Fev 2013].

TELEGRAPH, 2008. *Georgia: Russia conducting cyber* war [Em linha]. Londres: Telegraph.co.uk, 11 de Agosto 2008. Disponível em: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html, [Consult. 12 Nov. 2012].

TERRA,2012. *Armas digitais da ciberguerra.*[m linha]. Brasil, Disponível em: http://www.terra.com.br/noticias/tecnologia/infograficos/ciberguerra/, [Consult. 15 Jan. 2013]

WEF, 2013 : *Global risks 2013.*[Em linha]. Nova Iorque, Disponivel em: http://reports.weforum.org/global-risks-2013/view/section-one/methodology/, [Consul. 15 Abr. 2013].

ANEXO A-Caraterização dos tipos de ciberataques em 2012

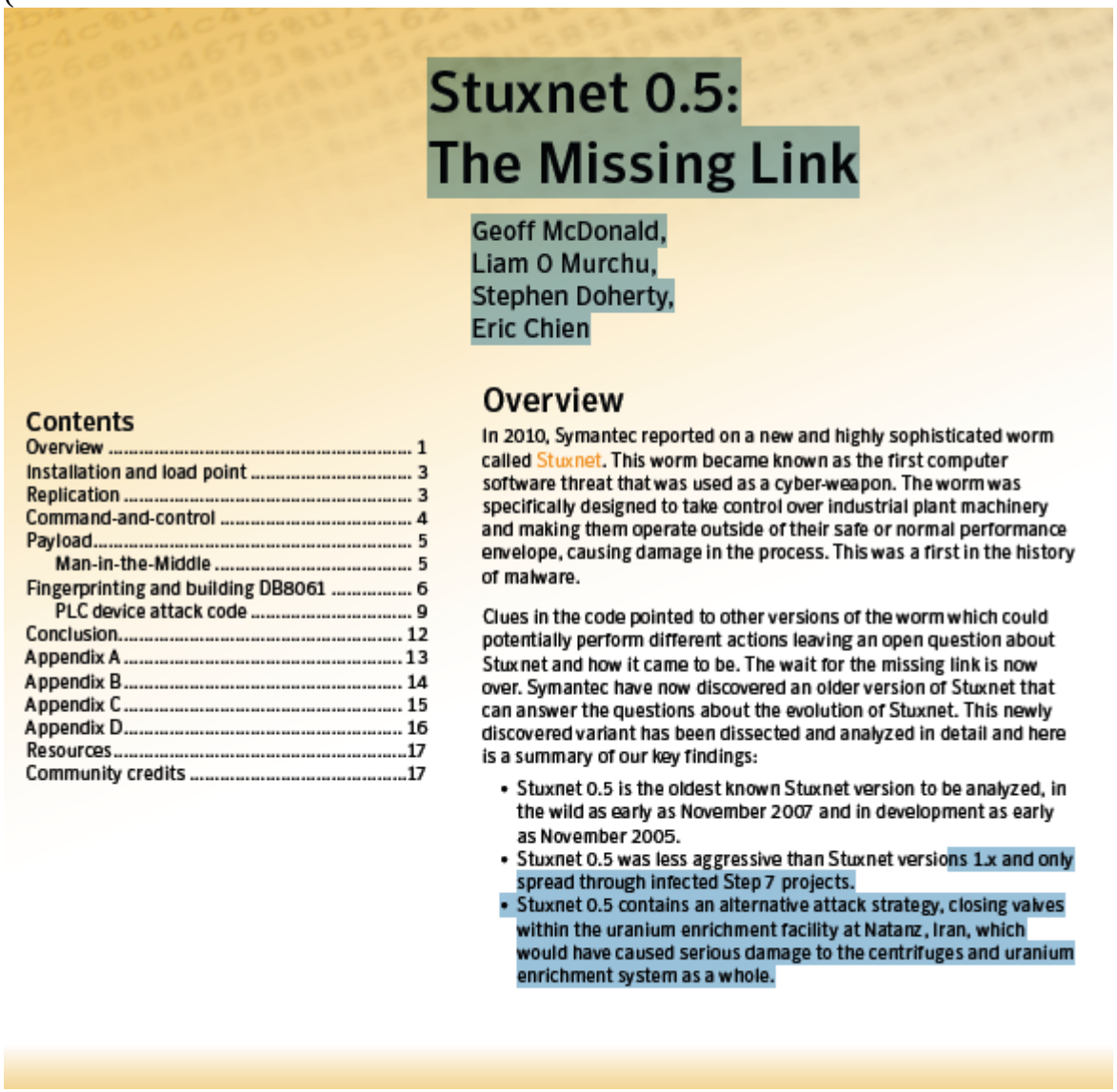
Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

Fonte: (ENISA , 2012)

Anexo B: Ficha técnica do vírus Stuxnet 0.5:The Missing Link

(



Stuxnet 0.5: The Missing Link

Geoff McDonald,
Liam O Murchu,
Stephen Doherty,
Eric Chien

Contents

Overview

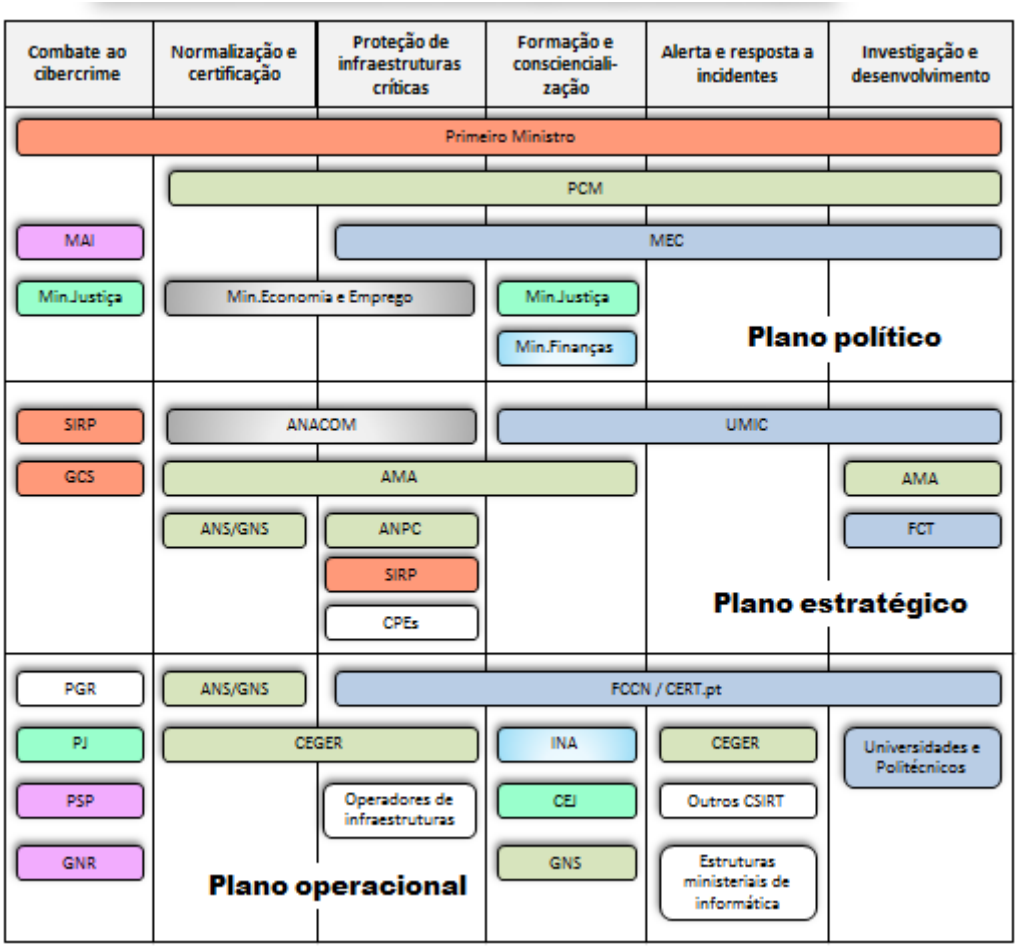
In 2010, Symantec reported on a new and highly sophisticated worm called Stuxnet. This worm became known as the first computer software threat that was used as a cyber-weapon. The worm was specifically designed to take control over industrial plant machinery and making them operate outside of their safe or normal performance envelope, causing damage in the process. This was a first in the history of malware.

Clues in the code pointed to other versions of the worm which could potentially perform different actions leaving an open question about Stuxnet and how it came to be. The wait for the missing link is now over. Symantec have now discovered an older version of Stuxnet that can answer the questions about the evolution of Stuxnet. This newly discovered variant has been dissected and analyzed in detail and here is a summary of our key findings:

- Stuxnet 0.5 is the oldest known Stuxnet version to be analyzed, in the wild as early as November 2007 and in development as early as November 2005.
- Stuxnet 0.5 was less aggressive than Stuxnet versions 1.x and only spread through infected Step 7 projects.
- Stuxnet 0.5 contains an alternative attack strategy, closing valves within the uranium enrichment facility at Natanz, Iran, which would have caused serious damage to the centrifuges and uranium enrichment system as a whole.

Fonte: (SYMANTEC, 2012)

Anexo C: Entidades relevantes na cibersegurança em Portugal



Fonte: (Santos , 2011)

Apêndice 1 - Diagrama de validação das hipóteses

Questão Central	Questões Derivadas	Hipóteses	Confirmação das Hipóteses	Resposta à Questão Central
De que forma as FFAA poderão desenvolver e aumentar a cooperação internacional na ciberdefesa?	**QD1**: Qual é a capacidade de ciberdefesa que já foi desenvolvida pelas FFAA?	**HIP1:** As FFAA dispõem de uma capacidade limitada na luta contra os ciberataques.	HIP1 validada. Página 23	As FFAA deverão aumentar as suas competências associadas à da capacidade de ciberdefesa, para que possam melhorar e aumentar a cooperação em novas áreas, da ciberdefesa.
	QD2: Como é que a capacidade de ciberdefesa já desenvolvida pelas FFAA, contribui para a cooperação internacional?	**HIP2**: A Cooperação entre as FFAA e outras organizações é reduzida	HIP2 validada. Página 31	
	QD3: Quais as áreas de cooperação internacional de ciberdefesa que são desejáveis pelas FFAA?	**HIP3:** Os ciberataques, não tendo fronteiras, exigem a definição de áreas comuns de cooperação internacional.	HIP3 validada. Página 40	
	QD4: Quais as componentes a desenvolver pelas FFAA que são necessárias para que se atinja a ciberdefesa cooperativa de forma desejável?	**HIP4:** As componentes a desenvolver no estabelecimento de uma ciberdefesa cooperativa internacional deverão permitir a partilha de informações técnicas, a normalização de procedimentos e a formação e treino.	HIP4 validada. Página 46	